ホ ー ル

群　論

(上)

金 沢　稔
八 牧 宏 美 訳

数 学 叢 書

10

吉 岡 書 店

THE THEORY OF GROUPS

by

Marshall Hall, Jr.

序　　文

本書は二重の目的をもって書かれている．初めの十章は群論の基本事項と各章の終りの演習問題からなり，後半の十章は群論を学ぶに際して参照事項として使用されるように書いてある．本書を教科書として使用する際は，Birkhoff, MacLane 共著の *A Survey of Modern Algebra* と同程度の現代代数学の知識をもった学生に適している．本書を著わすにあたって，できるかぎり必要事項をほとんど何の予備知識もなく読めるように努めたが，若干のやさしい予備知識が必要なときは上述の Birkhoff-MacLane の本を参照されたい．

Mathematical Reviews[1] に網羅された出版物をみて分かるように，現在の群論の研究は長足の進歩を遂げつつあるので，あらゆる事項を網羅することはもちろんのこと，完全な文献目録を与えることすら不可能である．それゆえ扱う事項を選ぶに際しては私自身の興味によりかなり左右され，また文献目録も本書に使用されたものにかぎって与えることにした．多大の興味をもつ事項でもその詳細な研究内容を既刊の出版物で容易に入手できるものについては努めて簡潔に著わすようにした．無限可換群の詳細な研究に対しては Kurosch 著の *Theory of Groups* の改訂版および Kaplansky の論文 *Infinite Abelian Groups* を参照されたい．また，鈴木通夫氏の論文 *Structure of a Group and the Structure of its Lattice of Subgroups* と Coxeter, Moser 共著の著書 *Generators and Relations for Discrete Groups* は，これらの事項をさらに深く研究されようとする読者におすすめできる文献である．

過去十年にわたってオハイオ州立大学において私が行なった群論の講義録をもとにして，それを発展させたのが本書であり，その主要部分はジョン・シモ

---

1)　ドイツ・フランスおよびソビエトの同種の雑誌と並んで，アメリカ数学会発行の月刊雑誌で，最近の数学論を世界各国の研究発刊物からとって紹介している有名な刊行物である．

ン・グッゲンハイム財団の研究費のもとで，1956年に滞在したケンブリッジのトゥリニティ大学で書き上げたものである．本書の発行を援助してくださった上記財団および種々の厚意を与えられたトゥリニティ大学の諸氏に感謝の意を表したい．

また原稿を準備するにあたって，数多くの有益な助言と未発表の研究すらご教示いただいたケンブリッジ王立大学の Philip Hall 教授にも多大の感謝の意を記さねばならない．Philip Hall 先生の多くのご親切を記念して本書を先生に献ずる次第である．

なお原稿に関して幾多の有益な助言をくださった Herbert J. Ryser 教授，Jan Korringa 教授および Ernest T. Parker 博士にも感謝の意を表したい．

Marshall Hall, Jr.

（オハイオ州 Columbus 市にて）

訳　者　序

著者の序文にもあるごとく最近の群論の分野における進歩は目を見張るばかりである．たとえば有限群論においては長年の懸案であった W. Burnside の予想“素数位数の fixed-point-free automorphism をもつ群は巾零である”および“奇数位数の群は可解である”はそれぞれ J. G. Thompson および W. Feit—J. G. Thompson（共著）により肯定的に解決され，また M. Suzuki, R. Ree, Z. Janko 等々による一連の新しい単純群の発見とその特徴づけなどがそれである．そのような状況におかれた我々にとっては，すでに古典的名著ともいわれている M. Hall の *The Theory of Groups* をじっくりと腰を据えて読むことにより将来への指針を見出せるのではなかろうか．この意味においてこの名著の飜訳は無視できぬ意義をもつように思われる．

さて，彌永昌吉先生から本書の飜訳についての話があったのは約二年半前のことであるが，多忙のため訳が進まず，さらに原稿半ばにして訳者二人が遠隔地に赴任し，その結果連絡も不十分になりがちで予定を約一年も遅れて脱稿に至った．読者諸氏および出版社に多大の御迷惑をかけたことをここに詫びるものである．

なお我々の稚拙な文章を通読され数々の有益な助言をいただいた岩堀長慶先生および出版に際してお世話になった吉岡書店の上川正司氏に感謝の意を表します．また多くの見落しや誤訳もあろうと思うが読者諸氏のご叱正を願う次第である．

1969年7月

訳　　者

目　　次

（上　巻）

下巻 主要目次

1), 2) ……は訳者註 *), **) は原著者註

第1章 基本事項

1.1. 代数法則

代数とは数のように加法，乗法あるいはその両者による算法をもつ元の集合を取り扱う学問である．与えられた系の元を文字 $a, b, c, \cdots$ で表わす．この系を $S=S(a, b, c, \cdots)$ で表わす．この系の性質は次の基本的な法則のどれが満たされているかに依存している．

閉　律

$A0$.　加法が定義可能である．

$M0$.　乗法が定義可能である．

すなわち，S の任意の順序づけられた元の対 a, b に対して $a+b=c$ となる S の元 c がただ一つ定まる．同じく $ab=d$ となる S の元 d がただ一つ定まる．

結合律

$A1$.　$(a+b)+c=a+(b+c)$

$M1$.　$(ab)c=a(bc)$

可換律

$A2$.　$b+a=a+b$

$M2$.　$ba=ab$

零および単位元

$A3$.　元 0 が存在して，任意の元 a に対して $0+a=a+0=a$ となる．

$M3$.　元 1 が存在して，任意の元 a に対して $1a=a1=a$ となる．

負元および逆元

$A4$.　任意の元 a に対して $(-a)+a=a+(-a)=0$ となる元 $-a$ が存在

する.

$M4$[1]. 零でない任意の元 a に対して $(a^{-1})a=a(a^{-1})=1$ となる元 a^{-1} が存在する.

分配律

$D1$. $a(b+c)=ab+ac$

$D2$. $(b+c)a=ba+ca$

定 義：$A1\sim A4$, $M1\sim M4$, $D1$, $D2$ を満足する系を体とよぶ. $A0$, $A1$, $A2$, $A3$, $A4$, $M0$ $M1$, そして $D1$, $D2$ を満足する系を環とよぶ.

公理系 $A0-A4$ は, $M4$ の0の逆元が存在しないことを除けば, 公理系 $M0-M4$ と全く平行な体系であることに注意しよう. $M0-M4$ での乗法を加法に書き改めたものが $A0-A4$ となるにすぎない. しかし分配律においては加法と乗法との挙動は全く異なるものである. 加法と乗法の間のこのような平行性は, 対数函数を用いる時に利用される. そこでの加法, 乗法間の基本的対応は次の法則で与えられる.

$$\log(xy)=\log x+\log y.$$

一般に一つの集合 S における n 項演算とは, S の n 個の元 $(a_1, \cdots, a_n)$ を変数とする函数 $f=f(a_1, \cdots, a_n)$ であって, その値 $b=f(a_1, \cdots, a_n)$ は S のただ一つの元となるようなものをいう. もし S の各元 $a_1, \cdots, a_n$ に対して $f(a_1, \cdots, a_n)$ が定義されるとき我々は演算 f が定義可能, または集合 S が演算 f に関して閉じているとよぶ.

体 F においては2項演算加法と乗法が定義可能であり, 一方, 逆元を取る演算 $f(a)=a^{-1}$ は, 0でないすべての元 a に対して定義される1項演算である.

1.2. 写 像

集合 S から集合 T の中への写像という概念は近代数学において基本的な概念

1) $M4$ は加法と乗法の両者が定義されている系で適用する. もし加法が定義されていないならば S には0が存在しない. そして法則は次のように改められうる. すべての元 a に対して $(a^{-1})a=a(a^{-1})=1$ となる元 a^{-1} が存在する.

である．

定　義：集合Sから集合Tの中への写像αとはSの各元xに対してただ一つのTの元yを対応させる規則のことである．記号で表わせば，

$$\alpha: x \to y \quad \text{または} \quad y=(x)\alpha.$$

元yをαによるxの像とよぶ．Tのすべての元yが少なくとも1個のSの元の像となっているときαをSからTの**上への**写像とよぶ．

一個の集合からそれ自身の中への（あるいは上への）写像は特に重要である．たとえば平面における回転は平面の点の集合からそれ自身の上への写像とみなされる．集合SからSの中への2個の写像 α, β の結合を定義する．

定　義：上の α, β に対してSからSの中への第3の写像γを次のように定義する．$y=(x)\alpha$, $z=(y)\beta$ ならば $z=(x)\gamma$．このγをαとβの積とよび $\gamma=\alpha\beta$ とかく．

ここで，$y=(x)\alpha$, $z=(y)\beta$ はただ一つ定まるから，$z=[(x)\alpha]\beta=(x)\gamma$ はすべてのxに対して定義されかつ，Sのただ一つの元として定まる．

定理 1.2.1. 写像の積を乗法とみなせば，集合SからSの中への写像の全体は $M0$, $M1$, $M3$ を満たす．

証：$M0$が成立することはすでに示した．$M1$について考えよう．α, β, γを3個の与えられた写像とする．Sの任意の元xを取り，$y=(x)\alpha$, $z=(y)\beta$, $w=(z)\gamma$ と置く．すると，$(x)[(\alpha\beta)\gamma]=z(\gamma)=w$, $(x)[\alpha(\beta\gamma)]=y(\beta\gamma)=w$．したがって二つの写像 $(\alpha\beta)\gamma$ と $\alpha(\beta\gamma)$ とはSの各元xに対して同じ像（image）をもつから $(\alpha\beta)\gamma=\alpha(\beta\gamma)$．また$M3$については$S$のすべての元を固定する写像を1で表わす．$(x)1=x$．するとすべての写像$\alpha$に対して $\alpha 1=1\alpha=\alpha$ となる．

一般には写像に対して $M2$ も $M4$ も成立しない．しかし，$M4$ はSからSの上への次の定義に述べる1対1の写像に対しては成立する．

定　義：集合Sから集合Tの上への写像αが１対１（しばしば1−1と書く）であるとは，Tのすべての元がSのただ一つの元の像となっていることである．この写像を $\alpha : x \leftrightarrows y$ で表わす．ここにxはSの元，yはTの元である．このときSとTは同じ濃度*) を持つという．

定理 1.2.2. 集合SからSの上への１対１の写像の全体は，$M0$, $M1$, $M3$, $M4$ を満足する．

証：定理 1.2.1. より $M0$, $M1$, $M3$ が成立することは分かる．したがって $M4$ が成立することを証明すればよい．$\alpha : x \leftrightarrows y$ とするとSのすべての元yに対して $y=(x)\alpha$ となるSの元xがただ一つ存在する．この対応は $\tau : y \leftrightarrows x$ を決める．τ の定義によって $(x)(\alpha\tau)=x, y(\tau\alpha)=y$ がSのすべての元 x, y に対して各々成立する．したがって $\alpha\tau=\tau\alpha=1$. このτが $M4$ における α^{-1} に等しい．

我々は一個の集合からそれ自身の上への１対１の写像を置換とよぶ．与えられた集合が有限のとき，集合の元を第１列に，その像を第２列に書くことによって置換を表わす．すなわち，$\alpha=\begin{pmatrix}1, 2, 3\\2, 3, 1\end{pmatrix}$, $\beta=\begin{pmatrix}1, 2, 3\\1, 3, 2\end{pmatrix}$ は集合 $S(1, 2, 3)$ 上の２個の置換である．その積は $\alpha\beta=\begin{pmatrix}1, 2, 3\\3, 2, 1\end{pmatrix}$ で定義される．ここで与えた置換の積の規約は左から右へ置換を順々に施すことであることに注意しよう．書物によっては積の定義が，乗法が右から左への順になっているのもある．

1.3. 群および関連のある代数系の定義

乗法も加法も一つの演算としての法則は同じである．ある集合からそれ自身の上への１対１の写像全体に対する積はこれらの法則のうち可換律を除けばすべてを満たしている．

定　義（群の第１の定義）：群とは元の集合 $G(a, b, c, \cdots)=G$ であって２元

*) 濃度については Birkhoff と MacLane [1] を参照のこと．この数字は末尾の参考文献の番号を表わす．（訳者注．参考文献は下巻末尾に掲載）

のあいだに積とよばれる演算が定義され次の法則を満足する．

$G0$. 閉律．Gの元の任意の順序づけられた組 a, b に対して $ab=c$ となるGの元がただ一つ定まる．

$G1$. 結合律．$(ab)c=a(bc)$.

$G2$. 単位元の存在．Gの任意の元aに対して $1a=a1=a$ となる元1が1個存在する．

$G3$. 逆元の存在．Gの任意の元aに対して $a^{-1}a=aa^{-1}=1$ となるGの元 a^{-1} が1個存在する．

$G2$, $G3$ の半分は不必要であり次の $G2^*$, $G3^*$ で置き換えられる．

$G2^*$. 1という元が存在して，Gの任意の元aに対して $1a=a$ を満たす．

$G3^*$. Gの任意の元aに対して，Gの元xが存在して $xa=1$ を満たす．

$G2^*$, $G3^*$ から $G2$, $G3$ を証明しよう．与えられた元aに対して $G3^*$ によって

$$xa=1 \quad \text{かつ} \quad yx=1$$

とする．すると

$$ax=1(ax)=(yx)(ax)=y[x(ax)]=y[1x]=yx=1,$$
$$a=1a=(ax)a=a(xa)=a1,$$

ゆえに $G2$, $G3$ が成立することが分かった．

単位元1と逆元 a^{-1} の一意性は容易に分かる．(問題13参照)．もちろん，$a1=a$, $ax=1$ を満たす1とxの存在性で $G2$, $G3$ を置き換えることができる．しかし，もし $a1=a$, $xa=1$ を満たす1とxの存在を仮定すれば状況は少々異なる*)．

順序づけられた列 $a_1a_2\cdots a_n$ を括弧でくくって値を算出する方法は沢山ある．$n=3$ に対しては $(a_1a_2)a_3$ と $a_1(a_2a_3)$ と丁度2通りの方法があるが結合律によって両者は等しい値を取る．結合律より次の重要な**一般結合律**が導かれる：

---

*) H. B. Mann [1]

順序づけられた列 $a_1a_2\cdots a_n$ をどのように括弧でくくって計算しても同じ値を得る．

この事実は n に関する帰納法を用いて容易に証明できる．（問題1参照）

単位元の存在を仮定しなくても群の定義を与えることはできる．

定　義（群の第2の定義）：$G=G(a, b, \cdots)$ が群であるとは次の 1)～4) を満足することである．

1)　G の任意の順序づけられた元 a, b に対して積 ab が定義され $ab=c$ となる G の元がただ一つ決まる．

2)　G の任意の元 a に対して G のただ一つの元 a^{-1} を定義する逆作用がある．

3)　結合律．$(ab)c=a(bc)$.

4)　逆律．$a^{-1}(ab)=b=(ba)a^{-1}$.

第1の定義を満たす集合が第2の定義を満たすことを示すのは容易である．第2の定義を仮定して第1の定義を導こう．

$$a^{-1}a=[(a^{-1}a)b]b^{-1}=(a^{-1}a)(bb^{-1})=a^{-1}[a(bb^{-1})]=bb^{-1}.$$

$a=b$ とすれば $a^{-1}a=aa^{-1}$．したがって G の任意の元 a に対して $a^{-1}a=aa^{-1}$ は G の一定の元である．この元を“1”とよぼう．$G3$ は成立する．また

$$1b=(a^{-1}a)b=a^{-1}(ab)=b$$
$$b1=b(aa^{-1})=(ba)a^{-1}=b$$

より $G2$ は成立する．ゆえに群に対する2個の定義は同値であることが分かった．別の定義を与えよう．

定　義（群の第3の定義）：集合 $G=G(a, b, \cdots)$ が群であるとは元のあいだの演算 a/b が定義されて，次の $L0$～$L4$ を満たすときである．

$L0$.　任意の順序づけられた組 a, b に対して，$a/b=c$ が G の元としてただ一つ定まる．

$L1$.　$a/a=b/b$.

$L2.$ $a/(b/b)=a.$

$L3.$ $(a/a)/(b/c)=c/b.$

$L4.$ $(a/c)/(b/c)=a/b.$

この演算に対して逆演算 b^{-1} を次の式で定義する.

$$b^{-1}=(b/b)/b$$

$L2$, $L3$ を使用して

$$(b^{-1})^{-1}=(b^{-1}/b^{-1})/b^{-1}=(b^{-1}/b^{-1})/[(b/b)/b]=b/(b/b)=b.$$

積を次の式で定義する.

$$ab=a/b^{-1}.$$

すると, $a/b=a/(b^{-1})^{-1}=ab^{-1}$. $L1$ を考慮して単位元1を $1=a/a$ で与えよう. したがって $L1$ より $aa^{-1}=1$ となる. それゆえ任意の a に対して $1=a^{-1}(a^{-1})^{-1}=a^{-1}a$. すなわち第1の定義の $G3$ が成立する. $b^{-1}=(b/b)/b$ において $b=1$ と置けば $1^{-1}=11^{-1}$ となるから, $1=1/1=11^{-1}=1^{-1}$. $L2$ より $a1^{-1}=a1=a$. $b^{-1}=1/b=1b^{-1}$, $b=a^{-1}$ より $(a^{-1})^{-1}=1(a^{-1})^{-1}$ すなわち $a=1a$. したがって第1の定義の $G2$ が成立する. $L3$ は $1(bc^{-1})^{-1}=cb^{-1}$ となるから $(bc^{-1})^{-1}=cb^{-1}$. $L4$ において $a=x$, $b=1$, $c=y^{-1}$と置けば $(xy)(1y)^{-1}=x1^{-1}=x$. すなわち $(xy)y^{-1}=x$. さて, 任意の x, y, z に対して, $a=xy, b=z^{-1}, c=y$ と置く. すると, $ac^{-1}=(xy)y^{-1}=x$, $L4$ より $(ac^{-1})(bc^{-1})^{-1}=ab^{-1}$ となる. ゆえに $(ac^{-1})(cb^{-1})=ab^{-1}$. x, y, z を用いて表わせば $x(yz)=(xy)z$, これは結合律 $G1$ が成立することを示している. ゆえに第3の定義から第1の定義が導かれた. 逆に第1の定義において $ab^{-1}=a/b$ と置けば, $L0$, $L1$, $L2$, $L3$, $L4$ が満たされることは容易に分かる. したがってこの2個の定義は同値であることが分かった.

群の公理の一部を満たす代数系を定義する.

定　義: 集合 $Q=Q(a, b, c, \cdots)$ が擬群 (quasi-group) であるとは2元の積 ab が定義され $ab=c$ において2元が定まれば第3の元がQの元としてただ一

つ定まるときである.

定　義：擬群が単位元1，すなわち $1a=a1=a$（各元 a に対して）なる元1をもつときループとよぶ.

定　義：集合 $S=S(a,b,c,\cdots)$ が半群（semi-group）であるとは2元の積 ab が定義され $(ab)c=a(bc)$ を満たすときである.

群は明らかにこれらの定義を満たす．Kurosch は半群かつ擬群である集合を群と定義した．実際半群は $G0$, $G1$ を満たす．ある元 b に対して $tb=b$ となるただ一つの元を t とする．元 b と a によって $by=a$ と定義される元を y とする．すると $(tb)y=by$，すなわち $ta=a$ が任意の元 a に対して成立するから $G2^*$ が満たされる．擬群において $G3^*$ は成立する．したがってこれらの性質は群を定義する.

積 ab と逆演算 a^{-1} をもつ集合があり，

$$a^{-1}(ab)=b=(ba)a^{-1}$$

を満たすならば，この集合を逆元をもつ擬群と呼ぶ．積が擬群を定義することを証明せねばならない．$ab=c$ と仮定すると $b=a^{-1}(ab)=a^{-1}c$，$a=(ab)b^{-1}=cb^{-1}$．したがって a と b は c を一意的に決める．与えられた c と a に対してたかだか1個の b が存在する．さらに与えられた c と b に対してたかだか1個の a が存在する．$a(a^{-1}c)=w$ とする．$a^{-1}[a(a^{-1}c)]=a^{-1}w$．ゆえに $a^{-1}c=a^{-1}w$．よって $(a^{-1})^{-1}(a^{-1}c)=(a^{-1})^{-1}(a^{-1}w)$ すなわち $c=w$ となる．ゆえに $a(a^{-1}c)=c$．同様にして $(cb^{-1})b=c$，したがってこの系は擬群となる．逆元をもつ擬群はループとはかぎらないことを注意しよう．3元 a,b,c と関係式 $a^2=a$，$ab=ba=c$，$b^2=b$，$bc=cb=a$，$c^2=c$，$ca=ac=b$ で各元はその元自身の逆元であることが分かる．しかも単位元を持たない擬群である.

1.4. 部分群，同型写像，準同型写像

群 G の元の部分集合 H が G の演算に関して群をなすとき H を部分群とよぶ.

任意の群Gにおいて単位元1は $1^2=1$ を満たす．逆にGの元xが $x^2=x$ を満たすと仮定する．$x=x^{-1}(x^2)=x^{-1}x=1$，すなわち部分群Hの単位元は大きな群Gの単位元に等しい．

定理 1.4.1. 群Gの空でない部分集合Hが部分群となるのは次の二つの条件が成立するときである．

$S1$. $h_1\in H$，$h_2\in H$ ならば $h_1h_2\in H$.

$S2$. $h_1\in H$ ならば $h_1^{-1}\in H$.

証：この二つの性質はHにおいて $G0$, $G2$, $G3$ が成立することを示している．Hにおける積はGにおける積と同じであるから $G1$ も成立する．

群のあいだにはいろいろな関係がある．まず第1に同型写像を定義しよう．

定　義：群Gの元から群Hの上への1対1の写像 $G\rightleftarrows H$ は，もし $g_1\leftrightarrows h_1$, $g_2\leftrightarrows h_2$，のとき，常に $g_1g_2\leftrightarrows h_1h_2$ が成立するならば同型写像とよぶ．

例 1. ある集合の上の置換の全体は定理 1. 2. 2 より群をつくるから，$S1$, $S2$ を満たす置換の集合は置換全体のなす群の部分群をつくる．例えば次のような部分群を考えよう．

G_1	G_2
$x_1=\begin{pmatrix}1,2,3\\1,2,3\end{pmatrix}$	$y_1=\begin{pmatrix}1,2,3,4,5,6\\1,2,3,4,5,6\end{pmatrix}$
$x_2=\begin{pmatrix}1,2,3\\2,3,1\end{pmatrix}$	$y_2=\begin{pmatrix}1,2,3,4,5,6\\2,3,1,6,4,5\end{pmatrix}$
$x_3=\begin{pmatrix}1,2,3\\3,1,2\end{pmatrix}$	$y_3=\begin{pmatrix}1,2,3,4,5,6\\3,1,2,5,6,4\end{pmatrix}$
$x_4=\begin{pmatrix}1,2,3\\1,3,2\end{pmatrix}$	$y_4=\begin{pmatrix}1,2,3,4,5,6\\4,5,6,1,2,3\end{pmatrix}$
$x_5=\begin{pmatrix}1,2,3\\3,2,1\end{pmatrix}$	$y_5=\begin{pmatrix}1,2,3,4,5,6\\5,6,4,3,1,2\end{pmatrix}$
$x_6=\begin{pmatrix}1,2,3\\2,1,3\end{pmatrix}$	$y_6=\begin{pmatrix}1,2,3,4,5,6\\6,4,5,2,3,1\end{pmatrix}$

G_1 の元 x_i を G_2 の元 y_i の上に写像すれば積が保たれることが分かる。したがって G_1 と G_2 は同型である．もっと一般にある群Gの元から他の群Hの元の上への写像があって積を保つときこの写像を**準同型**とよぶ．すなわち，

定　義：群Gの元から群Hの元の上への写像 $G\to H$ は，もし $g_1\to h_1$，$g_2\to h_2$ ならば常に $g_1g_2\to h_1h_2$ が成り立つとき準同型とよばれる．

準同型 $G\to H$ において1をGの単位元とする．Hの元eに対して $1\to e$ とする．すると $1^2\to e^2$，$1^2=1$ だから $e^2=e$．したがってeはHの単位元である．また $g\to h$，$g^{-1}\to k$ とすると $gg^{-1}\to hk$，ゆえに $1\to hk=e$．つまり $k=h^{-1}$．換言すればこの写像は逆元を逆元に移す．1対1の準同型写像は同型写像であることに注意しよう．

例 2. G_1 を上に述べた置換群，Hを実数1と -1 からなる乗法群とする．次の対応は準同型である．

$$x_1\to 1 \qquad x_4\to -1$$
$$x_2\to 1 \qquad x_5\to -1$$
$$x_3\to 1 \qquad x_6\to -1$$

置換群はそれ自身興味あるのみならず，すべての群は置換群と同型となる：

定理 1.4.2 (Cayley). すべての群はその元の上の置換群と同型である．

証：各元 $g\in G$，すべての元 $x\in G$ に対して，写像 $R(g): x\to xg$ を定義する．固定した元gに対してこの写像はGからGの上への写像となる．なぜならば与えられた元yに対して，$yg^{-1}\to(yg^{-1})g=y$ となるからである．$x_1g=x_2g$ とすれば $x_1=x_2$ となるからこの写像は1対1でもある．したがって各元gに対して $R(g)$ は置換を表わす．写像 $R(g_1)R(g_2)$ は $x\leftrightarrows x(g_1)g_2=x(g_1g_2)$ となるから $R(g_1)R(g_2)=R(g_1g_2)$．さらに $R(g_1)$ において $1\leftrightarrows g_1$, $R(g_2)$ において $1\leftrightarrows g_2$．つまり，もし $g_1\neq g_2$ ならば $R(g_1)\neq R(g_2)$，したがって $g\leftrightarrows R(g)$ は同型写像である．その上 $R(1)=I$ は単位写像，$R(g^{-1})R(g)=I$，ゆえに$R(g^{-1})=[R(g)]^{-1}$．

置換 $R(g): x \leftrightarrows xg$ はGの**右正則表現**とよばれる．また置換 $L(g): x \leftrightarrows gx$ をGの**左正則表現**とよぶ．$L(g)$ は逆同型写像である．これは写像 $L(g)$ が1対1かつ乗法が逆になることを意味する．すなわち $L(g_1g_2)=L(g_2)L(g_1)$.

添数集合JとGの部分群 $H_j(j\in J)$ の集合に対して，どの H_j にも属するGの元全体は S1, S2 を満たす．したがって部分群Hを形成する．このHを H_j の**共通部分**とよび $H=\bigcap_j H_j$ で表わす．有限個の積 $g_1\cdots g_s$ において各 g_i はある H_j に属するとき，これらの積全体の集合は S1, S2 を満たす．したがってこの集合は群Tを形成する．Tを H_j の**結び** (union) とよび $T=\bigcup_j H_j$ で表わす．2個の群HとKの共通部分および結びをそれぞれ $H\cap K$, $H\cup K$ で表わす．この記号は束論の記号と同じで第8章でもっと詳しく考えることにする．ある群の元の任意の集合を複体とよぶ．AとBが群Gの2個の複体であるとき ab, $a\in A$, $b\in B$ の形の元すべてからなる複体を AB で表わす．そして AB を AとBの積とよぶ．複体の積に対して結合律 $(AB)C=A(BC)$ が成立することは容易に分かる．Kを群Gの複体とする．Kの元またはKの元の逆元の有限個の積 $x_1\cdots x_n$ の全体からなる部分群を $\{K\}$ で表わす．$\{K\}$ はKで生成されるという．$\{K\}$ はKを含むGの任意の部分群に含まれることは容易に分かる[1]．

1.5. 剰余類. Lagrange の定理. 巡回群. 指数

群Gとその部分群Hが与えられたとする．Gの元xを固定したとき，hx, $h\in H$ とかける元の集合をHの**左剰余類**とよび，この集合を Hx で表わす．同様にして，xh, $h\in H$ とかける元の集合をHの**右剰余類**とよび xH で表わす．

定理 1.5.1. Gにおける2個のHの左（右）剰余類は共通部分が空であるか，または集合として一致している．Hの左(右)剰余類はHと同数の元を含む．

証：剰余類 Hx と Hy が元を共有しなければこの定理は成立する．したがって $z\in Hx$, $z\in Hy$ と仮定する．$z=h_1x=h_2y$ となる．$x=h_1^{-1}h_2y$, $hx=$

[1] すなわち $\{K\}$ は K を含む最小の部分群である．

$hh_1^{-1}h_2y=h'y$ より $Hx\subset Hy$. 同様にして $hy=hh_2^{-1}h_1x=h''x$ より $Hy\subset Hx$. ゆえに $Hx=Hy$. すなわち2個の集合は一致する. 右剰余類に対しても同様に証明できる. 対応 $h\leftrightarrows hx$, $h\leftrightarrows xh$, $h\in H$ はHと Hx, xH が同数の元を含んでいることを示している.

元 $x=x1=1x$ は剰余類 xH と Hx に属し, この剰余類の**代表元**とよばれる. 定理 1.5.1. より $Hu=Hx$, $u\in Hx$ であるから Hx の任意の元uは代表元に取ることができる. したがって $H=H1=1H$ はそれ自身剰余類の一つである. そして単位元が便宜上代表元に取られる.

$$G=H+Hx_2+\cdots+Hx_r \tag{1.5.1}$$

で剰余類 $H, Hx_2, \cdots, Hx_r$ はどの2個も共通部分がなく, 全体でGとなることを表わす. ここでの加法は便宜上の記号であって演算を表わすのではない.

$(Hx)^{-1}$・(hx という形の元の逆元の集合) は $x^{-1}H$ に等しく $(yH)^{-1}=Hy^{-1}$ だから左右の剰余類の間に1対1の対応が存在する. (1.5.1) より

$$G=H+x_2^{-1}H+\cdots+x_r^{-1}H. \tag{1.5.2}$$

部分群Hの左または右剰余類の個数はGにおけるHの指数とよばれ $(G:H)$ とかく. 群Gの位数とはGの元の個数のことである. 単位元はそれだけで部分群を構成する. その各剰余類は1個の元からなる. したがって群の位数は単位部分群の指数に等しい.

定理 1.5.2. (Lagrange の定理). 群Gの位数は部分群Hの位数とHのGにおける指数との積に等しい.

証: $r=(G:H)$ 個の互いに交わらないHのGにおける剰余類はHと同じ数の元を含む. それがHの位数である.

HがGの部分群, KがHの部分群とする. さらに

$$G=H+Hx_2+\cdots+Hx_s,$$
$$H=K+Ky_2+\cdots+Ky_r.$$

とすると, $g\in G$ に対して $g=hx_j, h\in H$, $h=ky_i$, $k\in K$, と一意的にかける.

したがって，GにおけるKの剰余類は $Ky_ix_j, i=1, \cdots, r, j=1, \cdots, s$, で与えられる．2個のそのような剰余類が一致するためには，それらはHの同じ剰余類に属さねばならない．つまり同じ x_j をもつ．右より x_j^{-1} を掛けることによってそれらは同じ y_i をもたねばならないことが分かる．ゆえにKのHにおける剰余類は Ky_ix_j で与えられ，これらはすべて相異なる．したがって次の定理が証明された．

定理 1.5.3. $G \supseteq H \supseteq K$, ならば $(G:K)=(G:H)(H:K)$.

群Gはその任意の元がある固定された元bの巾 b^i で表わせるとき**巡回群**とよばれる．$(b^{-1})^r=b^{-r}$ とかくと，結合律と帰納法によって $b^mb^t=b^{m+t}$ となることが分かる．ただし m, t は整数である．bの巾のすべてが互いに相異なるときこの巡回群は無限位数で，すべての整数がつくる加法群と同型になる．これらの整数は生成元bの巾指数である．$m>t$ に対して $b^m=b^t$ とすると $b^{m-t}=1$ かつ $m-t>0$. $b^n=1$ となる最小の正の整数をnとする．この群の元は $1, b, b^2, \cdots, b^{n-1}$ で $0 \leq r$, $s<n$ に対して $r+s<n$ ならば $b^rb^s=b^{r+s}$, $r+s \geq n$ ならば $b^rb^s=b^{r+s-n}$ となることが容易に分かる．このことから各正の整数nに対して位数nの巡回群が同型を除いてただ一つ定まることが分かる．これはnを法とする整数の加群である．したがって，1個の元bで生成された巡回群に対して，その位数は無限であるかまたはある正の整数nであり，ここでnは $b^n=1$ を満たす最小の正の整数である．我々は**元 b の位数**をbが生成する巡回群 $\{b\}$ の位数として定義する．

群Gの部分群の性質および個数はGの構造と密接な関係がある .しかしGが自分自身および単位群以外に部分群を含まなければGの構造を特徴づける真の部分群は存在しない．このときGの構造は非常に簡単になる．

定理 1.5.4. 群Gが単位群でないとする．Gが自分自身以外の部分群をもたないための必要十分条件はGが素数位数の有限巡回群となることである．

証：仮定よりGの1と異なる元bを取る．bから生成された巡回群はGと一致する．bの位数が無限とすればb^2は真の部分群を生成する．その元は b^{2j} 違

からなる．したがって b の位数 n は有限である：$b^n=1$．n が素数でないと仮定すれば $n=uv$, $v>1$, $u>1$ とかける．しかも b^u は位数 v の真の部分群を生成する．ゆえに n は素数で G は素数位数の巡回群となる．Lagrange の定理より素数位数の群は単位群および自分自身以外の部分群を含むことはできない．

部分群の指数に関する基本的な関係がある．

定理 1.5.5.（指数に関する不等式）． $(A\cup B:B)\geq(A:A\cap B)$.

証：$A\cap B=D$, $A=D1+Dx_2+\cdots+Dx_r$ とする．剰余類 $B1, Bx_2, \cdots, Bx_r$ が $A\cup B$ の中ですべて相異なることを示せばよい．$j\neq i$ に対して $Bx_i=Bx_j$ とすれば $x_j=bx_i$, $b\in B$．しかし，x_i, x_j はどちらも A に属しているから b も A に属する．したがって $b\in A\cap B=D$；剰余類 Dx_j と Dx_i は元 $x_j=bx_i$ を共有する．これは仮定に反する．ゆえに $A\cup B$ における B の剰余類の数の方が A における $A\cap B$ の剰余類の数より多いかまたは等しい．不等式が証明された．

定理 1.5.6.（指数等式）． $(A\cup B:B)$, $(A\cup B:A)$ が有限かつ互いに素とする．すると $(A\cup B:B)=(A:A\cap B)$, $(A\cup B:A)=(B:A\cap B)$.

証：定理 1.5.3. より $(A\cup B:A\cap B)=(A\cup B:B)(B:A\cap B)=(A\cup B:A)(A:A\cap B)$, 定理 1.5.5. より $(A\cup B:B)\geq(A:A\cap B)$．しかし上の関係式より $(A\cup B:A)$ と $(A\cup B:B)$ は互いに素だから $(A\cup B:B)$ は $(A:A\cap B)$ を割り切る．したがって $(A\cup B:B)=(A:A\cap B)$, 同様にして $(A\cup B:A)=(B:A\cap B)$.

1.6. 共　役　と　類

G を群，S を G の元の任意の部分集合とする．固定した元 x に対して $x^{-1}sx$, $s\in S$ の形の元の集合 S' は x による S の変換とよばれ，$S'=x^{-1}Sx$ または $S'=S^x$ とかく．

補題 1.6.1. SとS^x濃度は等しい.

証：$s \to x^{-1}sx = s'$ は写像であるから $s' \to xs'x^{-1} = x(x^{-1}sx)x^{-1} = s$ も写像である．したがって $s \leftrightarrows x^{-1}sx$ は1対1の対応である．

SとS'はGの部分集合としHをGのある部分群，$S'=S^x$ となるHの元xが存在するときSとS'はHで共役とよぶ．$S'=x^{-1}Sx$ とする．$S=(x^{-1})^{-1}S'x^{-1}$. さらに $S''=y^{-1}S'y$ とすれば $S''=y^{-1}x^{-1}Sxy=(xy)^{-1}S(xy)$. $S=1^{-1}S1$. したがってHで共役という関係は反射的，対称的，かつ推移的であるから同値関係である．与えられたSと共役なものS'の全体を共役の類とよぶ．$(x^{-1}sx)^{-1}=x^{-1}s^{-1}x$ より $x^{-1}s_1x\cdot x^{-1}s_2x=x^{-1}(s_1s_2)x$. ゆえに次の補題が得られた．

補題 1.6.2. 部分群と共役な集合は再び部分群である.

もし $x^{-1}Sx=S$ ならば $S=xSx^{-1}$, $y^{-1}Sy=S$ とすれば $(xy)^{-1}S(xy)=S$, したがってHの元xで $S^x=S$ となるもの全体はHの部分群をなす．それをHにおけるSの**正規化群**とよび $N_H(S)$ で表わす．Hの元xでSの任意の元sに対して $x^{-1}sx=s$ となるもの全体は同様にしてHの部分群をなす．それをHにおけるSの**中心化群**とよび $C_H(S)$ で表わす．(ドイツ式にかけば $Z_H(S)$ とかく)．Sがただ一つの元からなるときは中心化群と正規化群は一致することに注意しよう．そして常に $C_H(S)\subseteq N_H(S)$ が成り立つ．$H=G$ のとき単にSの正規化群または中心化群とよぶ．GのGにおける中心化群ZをGの**中心**とよぶ．

定理 1.6.1. HでSと共役な集合の個数は $(H:N_H(S))$ に等しい.

証：$N_H(S)=D$ と置く．

$$H=D+Dx_2+\cdots+Dx_r \quad r=(H:N_H(S)).$$

すると $x, y\in H$ に対して $x^{-1}Sx=y^{-1}Sy$ となるための必要十分条件は $S=(yx^{-1})^{-1}S(yx^{-1})$ である．すなわち $yx^{-1}\in D$, $y\in Dx$. それゆえSとHで共役な2個の集合が一致する必要十分条件はSを変換する元がDの同じ左剰余類にはいることである．したがってHのもとでSと共役な集合の個数はDのHに

ける指数に等しい．

Sがただ一つの元sからなるときGで共役な元全体は1個の類をなす．Gにおける元の類はGの元の分割である．そして，

$$G=C_1+C_2+\cdots+C_s \tag{1.6.1}$$

とかく．$i \neq j$に対して$C_i \cap C_j=\phi$，かつGの各元はどれかただ一つの類C_iに属する．単位元1はそれだけで類をなす．定理1.6.1.より類C_iの元の数はある部分群の指数に等しいから群Gの位数の約数である．

1.7. 両側剰余類

与えられた群Gと2個の部分群HとK，Gの固定元xに対してHxKとかける元の集合を両側剰余類とよぶ．HとKは一致してもよい．普通の剰余類のときと同様に次の補題が成立する．

補題 1.7.1. 2個の両側剰余類HxKとHyKは共通部分がないかまたは一致する．

証：$z=h_1xk_1=h_2yk_2$とすると$hxk=hh_1^{-1}h_2yk_2k_1^{-1}k$，したがって$HxK \subset HyK$．同様にして$HyK \subset HxK$．

両側剰余類HxKはHxkという形のHのすべての左剰余類を含むし，hxKという形のKのすべての右剰余類を含む．さらにHxKはHの左剰余類のいくつか，Kの右剰余類のいくつかからなることは明らかである．

定理 1.7.1. HxKにおけるHの左剰余類の数は$(K:K \cap x^{-1}Hx)$，HxKにおけるKの右剰余類の数は$(x^{-1}Hx:K \cap x^{-1}Hx)$である．

証：$hxk \leftrightarrows x^{-1}hxk$によって$HxK$の元から$x^{-1}HxK$の元の中への1対1の対応をつくる．この対応は$HxK$における$H$の左剰余類$Hxk$と$x^{-1}HxK$における$x^{-1}Hx$の左剰余類$x^{-1}Hxk$との間の1対1対応を，そしてまた$HxK$における$K$の右剰余類$hxK$と$x^{-1}HxK$における$K$の右剰余類$x^{-1}hxK$の

間の1対1対応を与える．$x^{-1}Hx=A$，$A\cap K=D$ とかく．$A=1D+u_2D+\cdots+u_rD$，$r=(A:D)$ とすれば $u_i\in A$，それゆえ $K, u_2K, \cdots, u_rK$ は AK におけるKの右剰余類である．$u_iK=u_jK$ とすれば $u_i^{-1}u_j\in K$，しかし $u_i, u_j\in A$ より $u_i^{-1}u_j\in D$．したがって $u_iD=u_jD$ となる．$K, u_2K, \cdots, u_rK$ はすべて相異なる．AK におけるKの右剰余類は aK の形をしている．ただし $a\in A$ は $d\in D$ に対して u_id の形をしている．$u_idK=u_iK$，ゆえに AK におけるKの右剰余類の数は $(A:D)=(x^{-1}Hx:x^{-1}Hx\cap K)$．そして1対1の対応によってこれは HxK におけるKの右剰余類の数である．同様にして AK におけるAの左剰余類の数は $(K:D)=(K:x^{-1}Hx\cap K)$ である．そして1対1の対応によってこれは HxK におけるHの左剰余類の数に等しい．

1.8. 無限群に関するいくつかの注意

群に関する多くの定理はその群が有限であるか否かに関係しない．しかしいくつかの定理には有限群であるか無限群であるかによって本質的に異なるものがある．時によっては結果は同じでも証明の方法が異なるときもある．

無限群Gはいくつかの有限的な性質をそなえていることもある．この種の重要な性質を次に述べる．

1) Gは有限生成である．

2) Gは**周期的**である．すなわち，Gの元はすべて有限位数である．

3) Gは**極大条件**を満たす．すべての互いに異なる部分群の昇鎖 $A_1\subset A_2\subset A_3\subset\cdots$ は有限でおわる．

4) Gは**極小条件**を満たす．すべての互いに異なる部分群の降鎖 $A_1\supset A_2\supset A_3\supset\cdots$ は有限でおわる．

無限群Gの性質がすべての有限生成の部分群に対して成立するとき，Gはこの性質を局所的にもつという．群Gの準同型像の類 H_i は，もしすべてのGの元 $g\neq 1$ に対して少なくとも1個の H_i が存在しそこでの g の像が単位元でないとき**残差類** (residual family) とよばれる．Gがある性質を残差的にもつとは，Gに対してこの性質を満たす準同型像の残差類が存在することをいう．

定理 1.8.1. 群Gが極大条件を満たす必要十分条件はGとそのすべての部分群が有限生成であることである.

証：HをGの部分群そして有限生成でないとする. Hの相異なる部分群の無限昇鎖をつくる.

$\{h_1\}\subset\{h_1, h_2\}\subset\cdots\subset\{h_1, \cdots, h_i\}\subset\cdots$ ここにおいて h_1 を任意にえらび h_i はHの元で $\{h_1, \cdots, h_{i-1}\}$ に含まれないものを取る. Hは有限生成な群 $\{h_1, \cdots, h_{i-1}\}$ とは異なるからこのような h_i は常に存在する. 逆にGとそのすべての部分群が有限生成であると仮定する. $B_1\subseteq B_2\subseteq B_3\subseteq\cdots$ をGにおける部分群の昇鎖とする. この列のある番号からあとの部分群がすべて等しくなることを証明し, 互いに異なる部分群の無限昇鎖が存在しないことを示そう. ある B_i に対して $b\in B_i$ となる元 b の全体はGの部分群Bをつくる. その理由は $b\in B_i$, $b'\in B_j$ ならば $k\geq i$, $k\geq j$ となるすべての B_k に b も b' も属し, それらの積も逆元も B_k に属するからである.

仮定によってBは有限個の元 $x_1, \cdots, x_n$ で生成される. x_1 を含むはじめての B_i を B_{j_1} で, そして一般に $k=1, \cdots, n$ に対して x_k を含むはじめての B_i を B_{j_k} とする. するともしmが $j_1, \cdots, j_n$ の中で最大であれば B_m は $x_1, \cdots, x_n$ のすべてを含む. それゆえ $B=B_m=B_{m+1}=\cdots$. 後で述べるが, 有限生成ではあるが有限生成でない部分群をもつ群がある.

定理 1.8.2. 極小条件を満たす群は周期的である.

証：Gが無限位数の元 b を含むとすれば, $\{b\}\supset\{b^2\}\supset\{b^4\}\supset\cdots\supset\{b^{2i}\}\supset\cdots$ は相異なる部分群の無限降鎖である.

無限群においてはその位数に関する有限の帰納法を用いることはできないので, 有限群に対して非常に有効なこの証明の方法に取って代わる方法が必要とされる. この別の方法の一つは集合と順序に関する非常に一般的な公理を必要とする. 元 $\{a, b, c, \cdots\}$ からなる集合Sにおいて順序 $a\leq b$ が定義されていると仮定しよう. その順序は次の公理のいくつかを満たす.

O1) $a\leq b$, $b\leq a$ ならば $a=b$.

$O2$) $a \leq b,\ b \leq c$ ならば $a \leq c$.

$O3$) 任意の2元 a, b に対して $a \leq b$ または $b \leq a$ のいずれかが成立する.

$O4$) Sの任意の空でない部分集合Tは最初の元 x_1 をもつ. すなわち $t \in T$ に対して $x_1 \leq t$ となる元のことである.

はじめの2個の公理が成立するとき, この順序は**半順序**であるという. はじめの3個の公理が成立するとき, この順序は**全順序**であるという. さらに4個の公理のすべてが成立するときこの順序を**整列順序**とよぶことにする. どんな集合にも4個の公理を満たすような順序づけが可能であると仮定する. すなわち**すべての集合 S は整列可能である**という公理を認める. $a \leq b$ かつ $a \neq b$ を $a < b$ で表わす. 整列順序集合において命題を**超限帰納法** (transfinite induction) で証明することができる. それは次のような方法である. Sの最初の元を1で表わす. $P(a)$ をSの元に関する命題とする. $P(1)$ が正しく, $x < a$ となるすべてのxに対して $P(x)$ が成立するならば $P(a)$ が成立するとき, すべての元 $b \in S$ に対して $P(b)$ が成立と結論する方法である. TをSの部分集合で $t \in T$ に対して $P(t)$ が不成立とする. Tが空集合でなければ最初の元cを含む. すると $c=1$ または $x < c$ となるすべてのxに対して$P(x)$は成立する. いずれにせよ $P(c)$ は成立することになりTからcをえらんだことに矛盾する. したがってTは空集合でSのすべての元bに対して $P(b)$ は成立する. 整列集合においては任意の降列 $a_1 > a_2 > a_3 > \cdots$ は必然的に有限でおわることに注意しておく.

論理的には整列可能の公理と同値である別の公理は Zorn の補題である.

補題 1.8.1. (**Zorn の補題**). Sを部分順序集合とする. Sのすべての全順序部分集合がS中上界(下界)をもつと仮定する. するとSは極大元(極小元)をもつ. ここでUをSの部分集合とするときUの**上界** b とはUのすべての元uに対して $b \geq u$ となる元のことである. **極大元** w は w と異なる上界をもたない. 同様にして**下界**, **極小元**を定義する.

群Gの部分群の集合は A, B を部分群とするとき包含関係 $A \subset B$ によって

半順序集合をなす．部分群の全順序集合において，そこに登場するすべての元の集合は部分群を形成する．なぜならば g_1 がある群に g_2 が別のある群に含まれているならば，g_1 と g_2 はともに二つの部分群より大きな群に含まれることになり，g_1g_2, g_1^{-1}, g_2^{-1} も含まれることになるからである．このように Zorn の補題は群論または一般に抽象代数学における証明に有効である．

整列可能の公理と Zorn の補題は次の撰出公理と論理的に同値である．

撰出公理． 集合 S の部分集合の集まり $\{S_i\}$ の任意の族 F を取る．このとき F の元に対して定義され $f(S_i)=a_i\in S_i$ となる撰出函数 $f(S_i)$ が存在する．ただし S_i は空ではないとする．

撰出公理は逆説めいているため疑問視される．しかし集合 S が可算集合であれば，これら三つの原理は正しい．S が可算集合とは S の元と自然数 1, 2, 3, …, の間に１対１の対応がつくことである．それらは他の集合 S に対して，そしておそらくすべての定義可能な集合に対して，たとえ実数全体の集合が整列不能であっても，成立すると仮定できる．この本でこれらの原理の一つを使用するときは，すべての集合 S とは“公理が成立するすべての集合 S”を意味するものとする．

これらの方法の有効な応用は次の定理である．

定理 1.8.3. 群 G の１元を g, H を G の部分群で g を含まないものとする．すると，g を含まない部分群の中で極大なもの M が存在し，M は H を含む．

証：Zorn の補題を用いる．H を含み g を含まない部分群の集合は包含に関して部分順序集合をなす．これらの群の全順序集合の元は H を含むが g を含まない群を形成する．したがって H を含むが g を含まない極大な群 M が存在する．

この定理によって次の定理が容易に得られる．

定理 1.8.4. G を有限生成の群，H を G の真の部分群とする．すると G の極大部分群 M が存在し，H を含む．

証：G が $x_1, \cdots, x_m$ で生成されるとせよ．$x_1, \cdots, x_m$ の中で H に含まれない

最初の元を y_1 とする．y_1 を含まない群の中で極大なものを M_1 とし，$M_1 \supseteq H$ とする．するとGの部分群で M_1 を真に含むものは y_1 を含む．$H_1=\{M_1, y_1\}$ と置く．$H_1=G$ ならば M_1 が求めるものである．$H_1 \neq G$ ならば，$x_1, \cdots, x_m$ の中で H_1 に含まれない最初の元 y_2 を含まない部分群の中で極大なもの M_2 を取り $M_2 \supseteq H_1$ とする．$G=\{x_1, \cdots, x_m\}$ だからこの操作を繰り返すことによって $M_i \supseteq H_{i-1} \supseteq \cdots \supseteq H$, $\{M_i, y_i\}=G$ となり，$M_i=M$ が求める極大部分群となる．

1.9. 群　の　例

ある集合からそれ自身の上へのある性質を保存する1対1の写像は常に群を形成する．興味のある群の大部分はこの方法で生ずる．幾何学的図形の合同変換はこの種のものである．合同変換とは，図形を自分自身上に写す写像であって，距離を変えぬものをいう．次のはじめの2個の例は合同変換の群である．

例 1. 二面体群[1]　辺の数 $n \geqq 3$ の正多角形の合同変換の全体は位数 $2n$ の群をなす．これらは頂点の動き方によって完全に決定される．頂点に時計の向きに $1, 2, \cdots, n$ と番号をつける．頂点1は頂点 $1, 2, \cdots, n$ のどれかの上に写像される．残りの頂点は時計の向き，または逆の向きに位置をしめる．すべての折り返しは回転

$$a=\begin{pmatrix}1, 2, 3, \cdots, n-1, n\\ 2, 3, 4, \cdots\cdots, n, 1\end{pmatrix}$$

と鏡映

$$b=\begin{pmatrix}1, 2, 3, \cdots\cdots, n-1, n\\ 1, n, n-1, \cdots\cdots, 3, 2\end{pmatrix}$$

によって生成される．$a^n=1$, $b^2=1$, $ba=a^{-1}b$．さらにこれらの関係は群を完全に決定する．なぜならば，a と b によって生成された群のすべての元は $a^{i_1}b^{j_1} \cdots a^{i_r}b^{j_r}$ の形であり $ba^i=a^{-i}b$ によって a^i または a^ib, $i=0, 1, \cdots, n-1$ の形にすることができるからである．すなわちこれらは $2n$ 個の異なった元である．これらの関係は $n=2$ に対しても群を定義し，それを四元群とよぶ．

---

[1] dihedral group とよばれる．

例 2. 立方体の合同変換の群 この群は8個の頂点からそれ自身の上への写像によって決定される．図のように符号をつける．この群は回転，

$$a=\begin{pmatrix}1, 2, 3, 4, 5, 6, 7, 8\\2, 3, 4, 1, 6, 7, 8, 5\end{pmatrix}$$

$$b=\begin{pmatrix}1, 2, 3, 4, 5, 6, 7, 8\\1, 4, 8, 5, 2, 3, 7, 6\end{pmatrix}$$

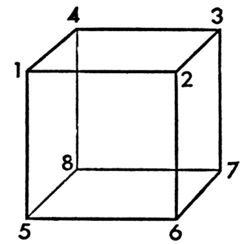


図 1. 立方体の合同変換の群

折り返し，

$$c=\begin{pmatrix}1, 2, 3, 4, 5, 6, 7, 8\\5, 6, 7, 8, 1, 2, 3, 4\end{pmatrix}$$

を含む．元 a, b はすべての頂点を他の頂点に移す群 G_1 を生成する．このことは次の図式より分かる．

$$1\xrightarrow{a}2\xrightarrow{a}3\xrightarrow{a}4\xrightarrow{b}5\xrightarrow{a}6\xrightarrow{a}7\xrightarrow{a}8\xrightarrow{a}5\xrightarrow{b}2\xrightarrow{a^{-1}}1.$$

$i\xrightarrow{x}j$ は元 x が i を j に移すことを意味する．このことから ba^2 は4を7に移す．1を固定する元は部分群 H_1 を形成する．そして，

$$G_1=H_1+H_1x_2+H_1x_3+H_1x_4+H_1x_5+H_1x_6+H_1x_7+H_1x_8,$$

ここで x_i は1を i に移す元である．x_i を次のようにえらぶことができる．$x_2=a$, $x_3=a^2$, $x_4=a^3$, $x_5=a^3b$, $x_6=a^3ba$, $x_1=a^3ba^2$, $x_8=a^3ba^3$．全部で8文字存在し剰余類 H_1x_i のすべての元は1を同じ文字 i に移す．そしてこれは H_1 のすべての剰余類を含む．そして H_1 の G_1 における指数は8である．

頂点1を固定する立方体の回転は隣接した3個の頂点を巡回的に置換せねばならない．したがって H_1 は位数3で $1, b, b^2$ のみを含むから G_1 は位数24である．折り返し c は G_1 には含まれないが，$c^2=1$, $ca=ac$, $cb=a^2ba^2c$ より a, b, c で生成された群 G は $G=G_1+G_1c$ となり位数48である．

例 3. 関係式

$$a^7=1,\quad b^3=1,\quad ba=a^rb$$

を満たす元 a, b で生成される群 G の位数はいくらか．G のすべての元は a および b の有限個の積で表わすことができる．$ba=a^rb$ によってどんな b も必ず

a のあとにくるようにできる．したがってすべての元は

$$g=a^ib^j \quad i=0,1,\cdots,6\ ; \quad j=0,1,2.$$

の形に書くことができる．この事実より G の位数はたかだか 21 であることが分かる．しかし実際の位数は関係式 $ba=a^rb$ における r の値に依存する．$ba^2=a^rba=a^r(a^rb)=a^{2r}b$, $ba^i=a^{ir}b$ となることが分かる．したがって $b^2a=ba^rb=a^{r^2}b$, $b^2a^i=a^{ir^2}b^2$ となる．ゆえに $b^3a=ba^{r^2}b^2=a^{r^3}b^3$. $b^3=1$ より $a=a^{r^3}$；したがって $a^7=1$. $r=1,2,3,4,5,6$ の中で $r=3,5,6$ に対しては $a=1$. そしてこの群は $b^3=1$ によって与えられる位数 3 の巡回群にすぎない．しかし $r=1,2,4$ に対しては結果は異なる．$r=1$ のとき $ba=ab=c$ は位数 21 の元である．逆に位数 21 の巡回群 $c^{21}=1$ において $b=c^7$, $a=c^{-6}$ とすれば $a^7=1$, $b^3=1$, $ba=ab=c$. $r=2$ のとき次の置換が働いている．

$$a=\begin{pmatrix}1,2,3,4,5,6,7\\2,3,4,5,6,7,1\end{pmatrix}$$

$$b=\begin{pmatrix}1,2,3,4,5,6,7\\1,5,2,6,3,7,4\end{pmatrix}$$

$r=4$ のとき，a に対しては同じ置換が，b に対しては第 2 の置換の逆元が働いている．群の定義の式を少し変えると群の構造がはなはだしく変わることをこの例は示している．

例 4. 7 文字 A,B,C,D,E,F,G の上の置換群であって次の図の列を置換するものを見つけよう．列における文字の順序は問題ではない．

$$\begin{matrix}A, B, C, D, E, F, G\\B, C, D, E, F, G, A\\D, E, F, G, A, B, C\end{matrix}$$

置換

$$a=\begin{pmatrix}A, B, C, D, E, F, G\\B, C, D, E, F, G, A\end{pmatrix}$$

は列を巡回的に置換する．もし G が置換の全体の群で H が第 1 列を固定する部分群であれば剰余類 Ha^i, $i=1,\cdots,6$ は第 1 列を第 $i+1$ 列の上に移す元全体からなる．それゆえ，

$$G=H+\cdots+Ha^6,\ (G:H)=7$$

Hの中に A, B, D を巡回的にうごかす元がある． A, B, D を巡回的にうごかすとき残りの文字のうごきを決めはしないが，もしCが固定されたとすれば置換は完全に決定されて

$$b=\begin{pmatrix} A, & B, & C, & D, & E, & F, & G \\ B, & D, & C, & A, & F, & G, & E \end{pmatrix}$$

となる．したがってもしKが第1列を固定し，さらに文字Aを固定する部分群であれば

$$H=K+Kb+Kb^2,\ b^3=1,\ (H:K)=3.$$

Kの中でBとDを交換する元をさがそう．

$$c=\begin{pmatrix} A, & B, & C, & D, & E, & F, & G \\ A, & D, & C, & B, & F, & E, & G \end{pmatrix}$$

もしTが A, B, D を固定する部分群であれば

$$K=T+Tc,\ c^2=1,\ (K:T)=2,$$

Tによって3文字A, B, Dが固定され，文字Cは C, E, F, G のどれかに移る．すなわち，

$$\begin{pmatrix} A, & B, & C, & D, & E, & F, & G \\ A, & B, & C, & D, & E, & F, & G \end{pmatrix}$$

$$\begin{pmatrix} A, & B, & C, & D, & E, & F, & G \\ A, & B, & E, & D, & C, & G, & F \end{pmatrix}$$

$$\begin{pmatrix} A, & B, & C, & D, & E, & F, & G \\ A, & B, & F, & D, & G, & C, & E \end{pmatrix}$$

$$\begin{pmatrix} A, & B, & C, & D, & E, & F, & G \\ A, & B, & G, & D, & F, & E, & C \end{pmatrix}$$

したがってTは位数4, Kは位数8, Hは位数24, そしてGは位数168となる[1)]．7文字 $A, \cdots, G$ を点と， 列を直線とみなせばこの図は7点からなる有限射影平面を表わし，群Gは共線変換群である．

例 5. 四元数群　次の位数8の群はいろいろな意味において例外的な群であ

1) この群は標数2の素体上の3次の正則行列全体のなす群 $GL(3,2)$ と同一視できる．

る．その特殊な性質は 12.5 節で説明される．ここではこの群を乗法表あるいは Cayley 表（イギリスの数学者の名前）によって表わそう．左端に x_i をもつ行，上端に x_j をもつ列において (i, j) 成分は積 $x_k=x_ix_j$ を表わす．

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
x_1	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
x_2	x_2	x_5	x_4	x_7	x_6	x_1	x_8	x_3
x_3	x_3	x_8	x_5	x_2	x_7	x_4	x_1	x_6
x_4	x_4	x_3	x_6	x_5	x_8	x_7	x_2	x_1
x_5	x_5	x_6	x_7	x_8	x_1	x_2	x_3	x_4
x_6	x_6	x_1	x_8	x_3	x_2	x_5	x_4	x_7
x_7	x_7	x_4	x_1	x_6	x_3	x_8	x_5	x_2
x_8	x_8	x_7	x_2	x_1	x_4	x_3	x_6	x_5

この表において各 x_i がちょうど 1 回各行にそして各列に表われることから積 $ab=c$ において a, b, c のどれか 2 元は第 3 の元を一意的に決める．したがって上の表は疑群の乗法表である．表より $x_1x_i=x_jx_1=x_i$ だから $x_1=1$ は両側単位元でこの表はループを決定している．最後の 2 行を

x_7	x_7	x_4	x_2	x_1	x_3	x_8	x_6	x_5
x_8	x_8	x_7	x_1	x_6	x_4	x_3	x_5	x_2

で置き換えてもこれら二つの性質は保たれる．この表は群の乗法表であることが示せるがそのためには結合律 $(ab)c=a(bc)$ をたしかめる必要がある．結合律をすべてたしかめるにはこの場合 $8^3=512$ 通り調べねばならない．a, b, c のどれか 1 個が単位元のとき $(ab)c=a(bc)$ が成立することをたしかめるのは容易であるがまだ343通り調べねばならない．ここで Cayley の定理 1.4.1 の逆を必要とする．

定理 1.9.1 (Cayley の定理の逆)．右正則表現 $x\to xg$ が群を形成するときループは群となる．

証：$R(g)R(h)$ によって $1\to g\to gh$, $R(gh)$ によって $1\to gh$. これは 1 を gh に移すただ一つの写像である．したがって $R(g)R(h)=R(gh)$. それゆえすべての x に対して $(xg)h=x(gh)$ となり結合律は成立する．

この場合 $a=x_2$, $b=x_3$ とかき

$$A=R(a)=\begin{pmatrix} x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 \\ x_2, x_5, x_8, x_3, x_6, x_1, x_4, x_7 \end{pmatrix}$$

$$B=R(b)=\begin{pmatrix} x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 \\ x_3, x_4, x_5, x_6, x_7, x_8, x_1, x_2 \end{pmatrix}$$

を計算する. $A^4=B^4=1$, $A^2=B^2$, $BA=A^3B$, そしてこれらの元は位数8の群を生成する. それは与えられたループの右正則表現でありそれゆえ群である. 置換の第2列は乗法表の列である. 生成元 a, b を用いて表わせば $x_1=1$, $x_2=a$, $x_3=b$, $x_4=ab$, $x_5=a^2=b^2$, $x_6=a^3$, $x_7=b^3=a^2b$, $x_8=a^3b$, また $a^4=1$, $b^4=1$, $b^2=a^2$, $ba=a^3b$ である.

演習問題

1. 結合律 $(ab)c=a(bc)$ を用いて $a_1a_2\cdots a_n$ のならぶ順序をかえずにどのように括弧でくくっても $a_1a_2\cdots a_n$ は同じ値を表わすことを証明せよ.
2. 任意の群において $(ab)^{-1}=b^{-1}a^{-1}$ が成立することを示せ. さらにもっと一般化して $(a_1a_2\cdots a_n)^{-1}=a_n{}^{-1}a_{n-1}{}^{-1}\cdots a_2{}^{-1}a_1{}^{-1}$ が成立することを証明せよ.
3. a と a^{-1} は位数が等しいことを証明せよ.
4. ab と ba は位数が等しいことを証明せよ. (ヒント: ab と ba は共役な元である.)
5. 正の整数 m, n に対して $a^m=1$, $b^n=1$ とする. k を m と n の最小公倍数とするとき $ab=ba$ ならば $(ab)^k=1$ となることを示せ. $ba\neq ab$ のとき $(ab)^k\neq 1$ となる例を見つけよ.
6. 群 G が位数2の元 a を唯一つもつとする. このとき G のすべての元 x に対して $xa=ax$ となることを証明せよ.
7. 共役類の個数が2である群は位数が2となることを証明せよ.
8. p, q が素数かつ $p<q$ ならば位数 pq の群は位数 q の部分群を唯一つもつことを証明せよ.
9. H を有限群 G の真部分群とする. H の共役の全体が G のすべての元を含むことはないことを証明せよ.
10. 位数 1, 2, 3, 4 のループは群であることを証明せよ. 位数5のループで群でないものを見出せ.
11. 両側剰余類 HxK は Hx と少くとも1元を共有する K の右剰余類のすべてを含むことを証明せよ.
12. (William Scott) 2項演算と, すべての元 a に対して $1a=a1=a$ となる単位元1をもつ集合は, $a_1a_2\cdots a_n$ の2通りの異なる括弧でくくったものが等しければ, 結合律

をみたすことを証明せよ．

13. 群の第1の定義から単位元1と逆元 a^{-1} の一意性を示せ．

14. A, B を群 G の2個の部分群とする．複体 AB はちょうど $(A:1)(B:1)/(A\cap B:1)$ 個の相異なる元を含むことを証明せよ．

第2章　正規部分群と準同型写像

2.1. 正規部分群

群Gの部分群HはGのすべての元xに対して，$x^{-1}Hx=H$ となるとき**正規部分群**とよぶ．1.6 の言葉を使えばGの部分群Hは $N_G(H)=G$ となるとき正規部分群である．

補題 2.1.1. 群Gの部分群HがGの正規部分群となる必要十分条件は左剰余類 Hx が右剰余類 xH となることである．

証：すべてのxに対して $x^{-1}Hx=H$ と仮定すると $Hx=xH$，逆に $Hx=yH$ とすれば $x\in yH$ より $yH=xH$．したがってすべての $x\in G$ に対して $Hx=xH$．それゆえ $x^{-1}Hx=H$.

系 2.2.1. 指数2の部分群は正規部分群である．

証：$G=H+Hx$ とすれば $G=H+xH$.

有限群に対して，$x^{-1}Hx\subseteq H$ ならば$x^{-1}Hx$とHの濃度は等しいので$x^{-1}Hx=H$ であるが，無限群に対してはこの包含関係から等号は成立しない．しかし，$x^{-1}Hx\subseteq H$，$xHx^{-1}\subseteq H$ ならば $H=x(x^{-1}Hx)x^{-1}\subseteq xHx^{-1}\subseteq H$．それゆえ $H=xHx^{-1}$，同様にして，$H=x^{-1}Hx$．したがってすべてのxに対して $x^{-1}Hx\subseteq H$ はHが正規となるために十分である．

真の正規部分群を含まない群は**単純**群といわれる．“単純”という言葉は術語として理解しなければならない．どんな真の部分群も持たない群は定理 1.5.4 より素数位数の巡回群である．これらの単純群は技術的にも，一般的な意味でも簡単である．しかし，他に非常に多くの単純群が存在する．たとえば 1.8 の第4の例にある位数168の群などである．有限単純群を決定する問

題[1] は未解決である．上にあげた素数位数の群を除いて，有限単純群の位数は偶数であると予想されているがこれは解決困難な問題のように思われる[2]．

2.2. 準同型の核

群Hが群Gの準同型像であると仮定する．Hの単位元の上に写像されるGのすべての元 $t\in G$ からなる集合Tを考えよう．

(2.2.1) $$G\to H,\ T\to 1$$

1.4 で注意したように $1\to 1$，だから $1\in T$．$t\to 1$，$t^{-1}\to u$ とすれば $1=tt^{-1}\to u$．しかし $1\to 1$ だから $u=1$，したがって $t^{-1}\to 1$ すなわち $t^{-1}\in T$．$t_1\to 1$，$t_2\to 1$，とすれば $t_1t_2\to 1$，より $t_1t_2\in T$．ゆえにTはGの部分群をなす．さらに $x\in G$，$t\in T$ ならば $x\to y$，$t\to 1$，$x^{-1}\to y^{-1}$，そして，$x^{-1}tx\to y^{-1}1y=1$．したがって $x^{-1}tx\in T$ となるからTはGの正規部分群である．この集合Tは準同型 $G\to H$ の**核** (kernel) とよばれる．

定理 2.2.1 (第1準同型定理)． 準同型 $G\to H$ においてHの単位元に写像されるGの元の集合はGの正規部分群をなす．Gの2元がHで同じ像を持つための必要十分条件は，この2元がTの同じ剰余類にはいることである．

証：Tが正規部分群となることはすでに示した．$x\to u$，$y\to u$，$x, y\in G$，$u\in H$ とする．$xy^{-1}\to 1$ より $xy^{-1}\in T$．それゆえ $x\in Ty$．xとyはTの同じ剰余類にはいる．逆に，$x\in Ty$ とすれば $x=ty$．もし $y\to u$ ならば $t\to 1$ だから $x\to u$，すなわちxとyはHにおいて同じ像を持つ．

2.3. 商　　　群

前節において準同型写像の核は群Gの正規部分群となることが示された．逆に，すべての正規部分群Tは準同型写像の核となる．実際にただ一つの準同型

---

1) 1960年代に入ってからも Suzuki, Janko, Held, Higman, Sims, Fisher 等によって新しい単純群が次々と発見されている．

2) Feit および Thompson によって肯定的に解決された．

写像の核になる．

$$(2.3.1)\qquad G=T+Tx_2+\cdots+Tx_r$$

TはGの正規部分群と仮定する．系Hの元として剰余類 Tx_i を取ろう．Hにおける積を，もし $x_ix_j\in Tx_k$ ならば

$$(2.3.2)\qquad (Tx_i)(Tx_j)=Tx_k$$

で定義する．

積が一意的に定義されることを示す必要がある．t_1x_i, t_2x_j をそれぞれ Tx_i, Tx_j の任意の元とする．T は正規部分群だから $t_1x_it_2x_j=t_1x_it_2x_i^{-1}\cdot x_ix_j=t_3x_ix_j$. しかし，もし $x_ix_j\in Tx_k$ ならば $t_3x_ix_j\in Tx_k$. したがって Tx_i と Tx_j の元のすべての積は同じ剰余類 Tx_k の元となる．ゆえに (2.3.2) における積は剰余類にのみ依存し代表元の取り方にはよらない．ゆえにHにおける積は定義される．

T は正規部分群だから $T^2=T$, $Tx_i=x_iT$. したがって，Hにおいて，$T\cdot Tx_i=Tx_i$, $Tx_i\cdot T=Tx_iT=TTx_i=Tx_i$ となって，T は単位元である．その上，$(Tx_iTx_j)Tx_k=Tx_ix_jx_k=Tx_i(Tx_jTx_h)$ となるなら，積は結合律を満たす．$x_i^{-1}\in Tx_j$ ならば Tx_iTx_j は $x_ix_i^{-1}=1$ を含む．$Tx_iTx_j=T$ よりHにおいて，$Tx_jTx_i=T$ も容易に分かるから Tx_j は Tx_i の逆元である．ゆえにHは群をなす．この群を**Tに関するGの商群**とよび $H=G/T$ とかく．

定理 2.3.1（第2準同型定理）． 群Gと正規部分群Tが与えられたとき，$H=G/T$ と置けば準同型 $G\to H$ でTを核とするものが存在する．この準同型は，$g\in Tx_i$ に対して $g\to Tx_i$ で与えられる．

証：$g\in Tx_i$ のとき，GからHの上への写像 $g\to Tx_i$ を考える．$g_1\in Tx_i$, $g_2\in Tx_j$, $x_ix_j\in Tx_k$ ならば，すでに示したように，$g_1g_2\in Tx_k$. したがって，$g_1g_2\to Tx_k=Tx_iTx_j$. ゆえにGからHの上へのこの写像は積を保つから準同型である．Tは G/T における単位元であるから $g\to 1(=T)$ となる必要十分条件は $g\in T$ である．ゆえに，Tはこの準同型の核である．証明は完了した．

定理 2.3.2（第3準同型定理）. $G \to K$がGからKの上への準同型，そして，Tをこの準同型の核とすればKは $G/T=H$ と同型になる．準同型 $G \to K$ において $x \to x^*$ であれば，$x^* \leftrightarrows Tx$ はKとHの間の同型写像を与える．

証：Gの元でTの同じ剰余類にはいる元はKにおいて，同じ像を持つから，$x^* \leftrightarrows Tx$ は1対1の対応である．$x \to x^*$，$y \to y^*$ とすれば $xy \to x^*y^*$．しかし $xy \in Txy$ より $x^*y^* \leftrightarrows Txy=TxTy$．したがって対応 $x^* \leftrightarrows Tx$ は積を保ち K と $H=G/T$ の間の同型写像である．

準同型定理に関するこれら三つの主要定理の内容を要約しよう．任意の準同型の核は正規部分群であり，任意の正規部分群は同型を除いて像がただ一つである準同型の核である．さらにこの像は与えられた群のその正規部分群に関する商群である．

定理 2.3.3. A, B を群Gの部分群とする．A, B のどちらか一方が正規部分群であれば $A \cup B = AB$.

証：有限個の元の任意の積 $x_1x_2\cdots x_s$，$x_i \in A$ またはB，が ab の形に書けることを示さねばならない．Bが正規部分群であれば $ba=aa^{-1}ba=ab'$，一方Aが正規部分群であれば $ba=bab^{-1}b=a'b$．したがって，どんな b も a の前にこないように積を書きあらわすことができる．積は $a_1a_2\cdots a_jb_{j+1}\cdots b_s=ab$ とかける．ここにおいて $a_i, a \in A$，$b_i, b \in B$ である．

定理 2.3.4. TをGの正規部分群とする．$H=G/T$ の部分群 K^* と，Gの部分群Kで $G \supseteq K \supseteq T$，となるものの間に1対1の対応がある．ここで$K$は$K^*$ の元の上に写像されるGのすべての元からなる．もし K^* がHで正規部分群であればKはGで正規部分群となる．この逆も成立する．また $(G:K)=(H:K^*)$ が成立する．

証：明らかにGの部分群のHにおける像は部分群をなす．K^* がHの部分群であればGにおける K^* の逆像Kは T，すなわち1の逆像を含む．また逆像は

群の公理を満足する．したがってHの部分群 K^* の逆像は $G \supseteq K \supseteq T$ を満たす唯一の部分群Kである．同じ K^* は準同型$G \to H$ においてKの唯一の像である．それゆえ $K \leftrightarrows K^*$ は$G \supseteq K \supseteq T$ と $H \supseteq K^* \supseteq 1$ の間の１対１対応である．K^* がHの正規部分群とすれば $x^{-1}Kx \to x^{*-1}K^*x^* = K^*$ より，すべてのxに対して $x^{-1}Kx \subseteq K$ となるからKはG中正規部分群である．もしKが正規部分群であればその像 K^* が正規部分群であることは明らかである．最後に剰余類 K^*g^* の逆像は剰余類 Kg であるから$(G:K)=(H:K^*)$となる．

もし任意の部分群Aが像 A^* をもてば A^* の逆像は $A \cup T = AT$ となることは容易に分かる．

2.4. 作　用　素

群GからGの中への写像 $\alpha : g \to g^\alpha$ は $(xy)^\alpha = x^\alpha y^\alpha$ となるときGの**自己準同型**またはGの**作用素**とよばれる．したがって自己準同型はGからGの中への準同型である．**自己同型**とはGからGの中への１対１自己準同型である．$g^\alpha = h^\alpha$ から $g=h$ が成立すれば自己準同型は同型であって，有限群においては必然的に自己同型となる．しかし無限群では真の部分群と同型になるかもしれない．$x \to 2x$ は有理整数の加法群の自己準同型であり，同型であるが，自己同型ではない．

Gの部分群Hはすべての自己準同型 α_i に対して $H^{\alpha_i} \subseteq H$ となるとき α_i に関して**認容**（admissible）といわれる．定義より認容部分群の和と共通部分は再び認容部分群となることは容易に分かる．さらに，作用αは認容部分群における作用とみることができる．しかし全体の群に対して異なる二つの作用が，認容部分群の上では一致することも生ずる．さらに $G \to K$ をGからKの上への準同型でその核Tが自己準同型αに関して認容ならば，Kに一つの作用素を定義することができる．

(2.4.1)　　$$(Tx)^\alpha = Tx^\alpha$$

と置く．剰余類 Tx に自己準同型をほどこすことは Tx^α に属するただ一つの

元を与えるからこれは自然な定義である．これがKにおける作用素を定義し，さらに準同型 $G\to K$ において $x\to x^*$ ならば $x^\alpha\to x^{*\alpha}$ となることは容易に確かめることができる．

二つの群AとBは，群の間の１対１対応 $A\leftrightarrows B$ と，作用素の間の対応 $\alpha_i\leftrightarrows\beta_i$ が存在して，$a\leftrightarrows b$ が同型写像とすれば，この対応において $a^{\alpha_i}\leftrightarrows b^{\beta_i}$ となるとき**作用同型**とよばれる．したがって作用同型は同型よりも強い意味を持つ．

定理 2.4.1. 群GとG上の作用域Ωが与えられたとする．AをGの認容部分群，TをGの認容正規部分群とする．すると $A\cap T$ はAの認容正規部分群となり，そして剰余群 $A\cup T/T$ と $A/A\cap T$ は作用同型である．

証：$A\cap T$ はΩ–部分群（すなわち Ω のもとで認容な部分群）の共通部分としてAのΩ–部分群である．$u\in A\cap T$，$a\in A$ とすれば $a^{-1}ua\in A$．またTはGの正規部分群で $u\in T$ だから $a^{-1}ua\in A\cap T$，したがって $A\cap T$ はAの正規部分群である．

$D=A\cap T$ とかく．

(2.4.2) $$A=D+Da_2+\cdots+Da_r$$

(2.4.2) で使ったように (2.4.3) において同じ剰余類の代表元を用いて次のようにかける．

(2.4.3) $$A\cup T=T+Ta_2+\cdots+Ta_r$$

$Ta_i=Ta_j$ とすれば $a_ia_j{}^{-1}\in T$．しかし $a_ia_j{}^{-1}\in A$ より $a_ia_j{}^{-1}\in A\cap T=D$，これは (2.4.2) に矛盾する．ゆえに (2.4.3) における剰余類はすべて異なる．さらにTは正規部分群だから $A\cup T=TA$，そして $A\cup T$ における任意のTの剰余類は $Ta=Tda_i$ の形をしている．ただし (2.4.2) より $a=da_i$ である．しかし $d\in T$ より $Tda_i=Ta_i$，それゆえ (2.4.3) における剰余類で $A\cup T$ はつきる．対応

(2.4.4) $$Da_i\leftrightarrows Ta_i$$

は（2.4.2）と（2.4.3）における剰余類の間の1対1の対応である．だから A/D の元と，$A\cup T/T$ の元の間の1対1の対応である．また，$d\in D$ に対して $a_ia_j=da_k$ ならば $D\subseteq T$ より $Da_iDa_j=Da_k$ かつ $Ta_iTa_j=Ta_k$．したがって対応（2.4.4）は剰余群 A/D と $A\cup T/T$ の間の同型写像である．作用素 $\alpha\in\Omega$ は，A/D と $A\cup T/T$ における作用を $(Da_i)^\alpha=Da_i{}^\alpha$，$(Ta_i)^\alpha=Ta_i{}^\alpha$ によって決定する．この方法によって与えられた作用に対して(2.4.4)が作用同型を与えることは容易に分かる．ゆえに証明は完了した．

群Gの部分群Kが正規部分群である必要十分条件は，Gの内部自己同型の類によってKが認容であることである．作用素を用いて部分群の正規性よりも強い形のものを定義する．群のすべての自己同型によって認容な部分群は**特性部分群**とよばれる．そしてすべての自己準同型で認容な部分群は**全不変部分群**とよばれる．したがって，群Gの中心Zは，すべての $g\in G$ に対して $zg=gz$ ならば自己同型αに対して $z^\alpha g^\alpha=g^\alpha z^\alpha$，そして$g$が$G$のすべての元をうごくとき g^α もGのすべての元をうごくので $z^\alpha\in Z$ となるから特性部分群である．しかし中心は全不変部分群とはかぎらない．たとえば，$a^4=1$，$b^2=c^2=1$，$ba=a^{-1}b$，$ca=ac$，$cb=bc$ で定義される位数16の群Gを考えよう．ここでは中心Zは a^2 と c で生成され位数4である．しかし写像 $a\to b$，$b\to c$，$c\to b$ はGの自己準同型を定義し，中心の元cを中心の外の元bの上に写像する．しかし自己準同型は元の形を保つ．それゆえすべての $x^3, x\in G$ またはすべての $x^{-1}y^{-1}xy, x, y\in G$ で生成された部分群は全不変である．

これらの正規性よりも強い形の特に重要な性質は次の事実である．群Gの正規部分群Kの正規部分群Hは一般にはGの正規部分群ではないが，特性部分群の特性部分群は定義より特性部分群である．さらに全不変部分群の全不変部分群は全不変部分群である．また正規部分群の特性部分群は正規部分群である．

2.5. 直積とカルテジアン積

与えられた群 A, B から，元の順序づけられた組 (a, b)，$a\in A$，$b\in B$ をつ

くることができる．これらの順序づけられた組は，積を

$$(a_1, b_1)(a_2, b_2)=(a_1a_2, b_1b_2) \tag{2.5.1}$$

と定義すれば新しい群，すなわち**直積**（direct product）$A\times B$ の元となる．すなわち，積の定義（2.5.1）は，AとBに対する群の公理のみから（1,1）を単位元とする群となることは容易に分かる．さらに対応 $(a,b)\leftrightarrows(b,a)$ より，$A\times B$ と $B\times A$ は同型であることが分かるからこれらの順序を無視して直積を考えることができる．対応 $a\leftrightarrows(a,1)$ はAと $A\times B$ において第2の成分を単位元とした集合との間の同型写像である．同様に，$b\leftrightarrows(1,b)$ はBと元$(1,b)$からなる部分群の間の同型写像である．さて，AとBをこれらの群と同一視しよう．この同一視によって$G=A\times B$はその部分群AとBの直積である．$(a,1)(1,b)=(a,b)=(1,b)(a,1)$ だから $A\times B$ においてAのすべての元はBのすべての元と**交換可能**である．すなわち $ab=ba$，$a\in A$，$b\in B$.

直積において $(a,b)^{-1}=(a^{-1},b^{-1})$，となるから，$(a_1,b_1)^{-1}(a_2,1)(a_1,b_1)=(a_1^{-1}a_2a_1,1)$，したがって$A$は $A\times B$ の正規部分群である．同様にしてBも $A\times B$ の正規部分群である．$(a,1)$，$(1,b)$ という形を同時に持つ元は $(1,1)$ であるから $A\cap B=1$．さらに $A\cup B$ はすべての積 $(a,1)(1,b)=(a,b)$ を含むから $A\cup B=A\times B$．AとBの間のこれらの関係は $A\times B$ を特徴づける．

定理 2.5.1. A,B が群Gの正規部分群で $G=A\cup B$ かつ $A\cap B=1$ ならばGは $A\times B$ に同型である．

証：直積 $A\times B$ において，部分群AとBはこの性質を満たすことはすでに示した．逆に A,B をGの正規部分群で $A\cap B=1$，$A\cup B=G$ と仮定する．$a\in A$，$b\in B$，に対して元 $a^{-1}b^{-1}ab=a^{-1}(b^{-1}ab)=(a^{-1}b^{-1}a)\,b$ を考えよう．AとBは正規部分群であるから，第一の括弧よりAの元であり，第2の括弧よりBの元である．これは $A\cap B=1$ の元である．ゆえに，$a^{-1}b^{-1}ab=1$，より $ab=ba$．定理 2.3.3，より $G=A\cup B=AB$ となるからすべての元gは $g=ab$ とかける．さらに $a_1b_1=a_2b_2$ より $a_2^{-1}a_1=b_2b_1^{-1}\in A\cap B=1$ となるから，この表わし方はただ一つしか存在しない．つまり $a_1=a_2$，$b_2=b_1$ となる．$g=ab$,

$g \leftrightarrows (a,b)$ としよう．$g_1=a_1b_1$, $g_2=a_2b_2$ ならば $g_1g_2=a_1b_1a_2b_2=(a_1a_2)(b_1b_2)$ したがって G と $A\times B$ の間の対応は1対1であるばかりでなく積を保存する．ゆえにGと $A\times B$ の間の同型写像が得られた．

我々は上の考えを一般化して，有限個または無限個の群の積を定義することができる．群の集合 $A_i, i\in I$ が与えられたと仮定する．i は添数集合 I をうごくとする．**形式的な積** $\prod_{i\in I} a_i$ をつくる．形式的な積とは各群 A_i から一元 a_i を選ぶことである．すべての形式的な積は A_i の**カルテジアン積**（Cartesian product）とよばれる群を形成する．ここで積はすべての $i\in I$ に対して

$$\prod_{i\in I} a_i \cdot \prod_{i\in I} b_i = \prod_{i\in I} c_i, \qquad (2.5.2)$$

$$c_i = a_ib_i$$

で定義する．

有限個の指数を除いてすべての $a_i=1$ となるカルテジアン積の部分群は A_i の**直積**とよばれる．明らかに因子の数が有限個のときには直積とカルテジアン積は一致する．いずれの場合にも $i\neq j$ に対して $a_i=1$ となる元 $\prod_i a_i$ は A_j と同型な正規部分群を形成しこの部分群を A_j と同一視する．すると $A_j\cap(\bigcup_{i\neq j} A_i)=1$. ここでは $\bigcup_{i\in I} A_i$ は直積である．

定理 2.5.2. 群Gが部分群 $A_i, i\in I$ の直積となる必要十分条件は，

1）すべての A_i が正規部分群である．

2）すべての $j\in I$ に対して $A_j\cap(\bigcup_{i\neq j} A_i)=1$.

3）$G=\bigcup_{i\in I} A_i$.

となることである．

証：証明は定理 2.5.1 の証明と深い関係がある．1）と 2）よりすべての a_i は $i\neq j$ なら a_i のすべての有限個の積と可換である．また 1)，2)，3）よりすべての $g\in G$ は A_i の元の有限個の積として表わすことができる．そして順序を除けば，各 A_i のたかだか1個の元を使うことによって一意的に表わすことができる．このことはGと A_i の直積との間の同型を与える．Gの元は

$g=1$ または $g=b_1\cdots b_m, b_k\neq 1, k=1,\cdots,m$, 各 b_i は異なる A_i に属するようにかくことができる. $b_k\in A_i$ のとき $a_i=b_k$, 他の場合には $a_i=1$ と置けば g には元 $\prod_{i\in I} a_i$ が対応する. この対応はGと A_i の直積との間の同型を与える.

演　習　問　題

1. すべての二面体群は位数2の群と準同型であることを証明せよ.
2. p,q が素数で $p<q$ ならば位数 pq の群の位数qの部分群は正規部分群であることを証明せよ.（第1章の演習問題8を見よ.）
3. 四元数群の部分群はすべて正規部分群であることを証明せよ.
4. 立方体において相対する面の中心を結ぶ3本の線分を x,y,z とする. 立方体の合同変換の群Gはこれらの線分を位数6の置換群Hの中でうごかすことを証明せよ. さらにHはGの準同型像であることを証明せよ.
5. 実数から実数の上への1対1の写像 $x\rightleftarrows ax+b, a, b$ は実数, $a\neq 0$, を考えよう. これらの写像は群Gを形成し, 変換 $T: x\leftrightarrows x+t$ は正規部分群をなすことを証明せよ.
6. 群Gの各元bに対して, 共役作用 $b: g\to g^b=b^{-1}gb$ を定義する. すべてのこのような作用に対してどの群が認容か. TがGの正規部分群のとき, $H=G/T$ に誘導された作用は再び共役作用であることを証明せよ.

第3章　アーベル群の基礎理論

3.1.　アーベル群の定義．巡回群

群Gが可換律

$$G4,\quad ba=ab,\quad a, b \text{ は} G \text{のすべての元}$$

を満たすとき，数学者 Abel の名をとって**アーベル群**とよばれる．$ba=ab$ のとき元aとbは可換であるという．

1.5 で一元bとその巾全体で生成された群として巡回群を定義した．$b^ib^j=b^jb^i=b^{i+j}$ がすべての整数i, jに対して成立するからすべての巡回群はアーベル群である．さらに 1.5 で同型を除いて無限位数のただ一つの巡回群と，位数nのただ一つの巡回群が存在することを注意した．巡回群のすべての部分群は巡回群である．このことを正確な形で証明しよう．

定理 3.1.1. 無限巡回群の単位群と異なるすべての部分群は有限指数の無限巡回群である．そして各有限指数に対してただ一つの部分群が存在する．位数nの有限巡回群のすべての部分群はnを割る位数の巡回群である．nを割る各位数に対してただ一つの部分群が存在する．

証：一元bで生成された巡回群Gとその部分群Hが与えられたとしよう．Hが単位群でなく，$b^i \in H$ とすれば $b^{-i} \in H$ かつiは正の整数である．Hの元の最小の正の巾をmとする．b^tをHの任意の元とすればrを適当に選ぶことによって $t=mr+s$, $0 \leq s < m$, $b^t=(b^m)^r b^s$. b^t, b^m はHにはいるから b^s もHの元である．sが0でなければmの定義に矛盾する．したがって $s=0$ かつ $b^t=(b^m)^r$, さらにHのすべての元は b^m の巾である．ゆえにHは巡回群である．任意の整数xに対して $x=km+i, i=0, 1, \cdots, m-1$, のいずれかであるから，

$$G=H+Hb+\cdots\cdots+Hb^{m-1} \tag{3.1.1}$$

等式 (3.1.1) はHのすべての剰余類を含む．そしてこれらはすべて異なる．その理由は $b^i=hb^j$, $i\neq j$, $0\leqslant i$, $j\leqslant m-1$, とすれば $b^{i-j}=h$ となり $|i-j|<m$ より $i=j$ となるからである．ゆえに $(G:H)=m$. ここでmはHの元でbの巾の最小の正の整数でありしかもHのGにおける指数である．したがってGが無限群であればすべての正のmに対して $(b^m)^r$ は部分群をなすから指数mの部分群がただ一つ存在する．Gが位数nの有限群であれば，$b^n=1$ かつ $n=mr$, m は n の約数となる．nを割る任意のmに対して $n=mr$ ならば元 $1, b^m, b^{2m}, \cdots, b^{(r-1)m}$, は位数$r$，指数$m$の部分群を形成する．$n=mr$ はnを2個の因子に分ける任意の方法であるから，nを割る各rに対して位数rの部分群がただ一つ存在することが分かった．

3.2. アーベル群の構造定理

無限アーベル群は非常に複雑な構造をもっている．比較的に簡単な例として，すべての複素数から零を除いたもののなす乗法群は有限位数と無限位数の元を含む．

$a^n=1$, $b^m=1$ がアーベル群で成立すれば，$(a^{-1})^n=1$, $(ab)^{mn}=1$ となるから，任意のアーベル群Aにおいて有限位数の元は部分群Fを形成する．Aのすべての自己準同型αは有限位数の元を有限位数の元の上に写像する．したがって2.4の意味でFはAの**全不変部分群**である．1.8で，すべての元の位数が有限である群を**周期群**とよんだ．これに対して，どんな元も単位元以外は有限位数でない群を**非周期群**とよぶ．

定理 3.2.1. アーベル群Aと有限位数の元からなるその部分群Fが与えられたとする．このとき A/F は非周期群である．

証：結果を否定して A/F の元 $x\neq 1$ が有限位数mであると仮定する．準同型 $A\rightarrow A/F$ において，$u\rightarrow x$ とする．すると $u^m\rightarrow x^m=1$. したがって $u^m\in F$ かつ u^m はある有限位数nである．$(u^m)^n=1$ よりu自身有限位数となる．ゆえに $u\in F$ かつ $u\rightarrow 1$, これは $x\neq 1$ に矛盾する．

この定理によってすべてのアーベル群を構成する問題は次の3個のもっとはっきりした問題に帰着される．

1)　すべての周期的アーベル群の決定．

2)　すべての非周期的アーベル群の決定．

3)　部分群として与えられた周期的群Fを持ち，Fによる剰余群が与えられた非周期的群と同型になるアーベル群Aの構成．

これらのどの一つも完全には解かれていないが，第一についてはほとんどのことが，最後の問題については少しのことが分かっている．

アーベル群Aにおいて元a_iの集合は，もし有限個の積$\prod_i a_i^{e_i}=1$がすべてのiに対して$a_i^{e_i}=1$のときにのみ成立するとき**独立**であるとよばれる．a_iが独立で，しかもAを生成するときa_iはAの**基底**であるという．したがって，元a_iがAの基底となるための必要十分条件はAがa_iで生成された巡回群の直積となることである．

アーベル群Aが元$a_1, \cdots, a_r$で生成されていると仮定する．するとAのすべての元はu_iを整数として$a_1^{u_1}\cdots a_r^{u_r}$の形に表わすことができる．もし

(3.2.1)
$$a_1^{x_1}\cdots a_r^{x_r}=1$$

が生成元のあいだの関係式ならば

(3.2.2)
$$a_1^{-x_1}\cdots a_r^{-x_r}=1$$

は逆の関係式とよばれる．Aで成立している関係式の集合SからSの関係式の積や逆元を取ることによって他の関係式を導くことができる．二つの関係式の集合S_1, S_2は各集合の関係式が他の集合の関係式から上のような方法によって得られるとき**同値**とよばれる．これは同値関係であることは容易に分かる．Aで成立するすべての関係式がSの関係式から得られるときこの集合SはAの**定義関係式**の集合とよばれる．生成元$a_1, \cdots, a_r$に関する関係の任意の集合Sは，Sから導かれる関係式は成立するが，他のものは成立しないような元$a_1, \cdots, a_r$，によって生成されたアーベル群の定義関係式の集合となることが示される．もちろん群Aは単位元だけになりうる．

定理 3.2.2. 有限個 r の元で生成されたアーベル群はたかだか r 個の元からなる基底を持つ.

証：$r=1$ に対してこの定理は明らかに正しい．なぜならば群が巡回群になるからである．A が $a_1, \cdots, a_r$ によって生成されると仮定する．証明は r と，固定した r に対して，関係式

(3.2.3) $$a_1^{x_1} \cdots a_r^{x_r} = 1$$

において $x_i = m$ となるような最小の正の整数 m に関する帰納法で行なう．すべての x_i が0となる関係式しか存在しなければ A は無限巡回群 $\{a_i\}$ の直積となって我々の定理は正しい．他の場合にはある関係式が存在して，ある正の巾を含んでいる．もし必要ならば a_i を並び換えて関係式における最小の正の巾が $x_1 = m$ となるようにする．$m=1$ ならば

(3.2.4) $$a_1 = a_2^{-x_2} \cdots a_r^{-x_r}$$

となって，A は $r-1$ 個の元 $a_2, \cdots, a_r$ で生成される．帰納法の仮定によって定理は正しい．関係式

(3.2.5) $$a_1^m a_2^{x_2} \cdots a_r^{x_r} = 1$$

において，$x_1 = m > 1$ と仮定する．$y_1, \cdots, y_r$ を他の関係式における巾とする．この関係式および (3.2.5) より任意の整数 k に対して巾が $y_1 - km$, $y_2 - kx_2$, $\cdots$, $y_r - kx_r$, の関係式が得られる．$0 \leqslant y_1 - km < m$ となるように k を選ぶことができる．しかし m は任意の関係式における最小の正の巾であったから，$y_1 - km = 0$, でなければならない．したがって巾が $y_1, \cdots, y_r$ の関係式は (3.2.5) と巾が 0, $y_2 - kx_2, \cdots, y_r - kx_r$, の関係式から得られる．ゆえに A に対するすべての関係式の集合は，(3.2.5) と $a_2, \cdots, a_r$ のみを含む関係式からなる集合 S と同値である．

(3.2.5) において $x_2 = k_2 m + s_2, \cdots, x_r = k_r m + s_r$ と置く．ここで $0 \leqslant s_i < m$ となるように $k_i, i = 2, \cdots, r$ を選ぶ．新しい元

(3.2.6) $$a_1^* = a_1 a_2^{k_2} \cdots a_r^{k_r}$$

を取れば $a_1^*, a_2, \cdots, a_r$ は A を生成する．そしてこれらの生成元を用いれば

(3.2.5) は

(3.2.7) $$a_1{}^{*m}a_2{}^{s_2}\cdots a_r{}^{s_r}=1$$

となる．もしすべての s が0でなければ，それはmより小さい正の数であるからここで帰納法の仮定を使うことができる．しかし，もし $s_2=\cdots=s_r=0$ ならば (3.2.7) は

(3.2.8) $$a_1{}^{*m}=1$$

となり，そして (3.2.5) と $a_2,\cdots,a_r$ だけを含む関係式は生成元 $a_1,a_2,\cdots,a_r$ のかわりのAに対する関係式の定義集合であるから，(3.2.8) と $a_2,\cdots,a_r$ のみを含んでいる関係式は，生成元 $a_1{}^*,a_2,\cdots,a_r$ のかわりの関係式の定義集合である．したがって，Aは $a_1{}^*$ で生成された位数mの巡回群と，$r-1$ 個の元 $a_2,\cdots,a_r$ で生成された群との直積である．後者は帰納法によってたかだか $r-1$ 個の巡回群の直積である．ゆえにすべての場合に我々の定理は証明された．

周期的アーベル群を研究するために，我々は任意の群において成立する補題を必要とする．

補題 3.2.1. n,m を互いに素な整数とする．xを任意の群の位数 mn の元とすれば，xは位数mの元yと位数nの元zを用いて $x=yz=zy$ と一意的に表わすことができる．yとzはどちらもxの巾である．

証：2個の整数 a,b の最大公約数を (a,b) で表わす．仮定より $(m,n)=1$. $um+vn=1$ となるような整数uとvが存在する．したがって，$x=x^{vn}x^{um}=x^{um}x^{vn}$. $y=x^{vn}$, $z=x^{um}$ と置く．すると $x=yz=zy$, かつ $y^m=x^{vnm}=1$, $z^n=x^{umn}=1$, yの位数 m_1 はmの約数である．さらに，zの位数 n_1 はnの約数である．しかし，$x=yz=zy$ よりxの位数は m_1n_1 の約数である．この位数は mn であるから $m_1=m$ はyの位数，$n_1=n$ はzの位数となる．もしxが他の表示 $x=y_1z_1=z_1y_1$, y_1 の位数 m, z_1 の位数n, となるものを持つとすれば $xy_1=y_1z_1y_1=y_1x$ かつ $xz_1=z_1y_1z_1=z_1x$ より，y_1 と z_1 はxと交換可能なことに注意しよう．しかしそれゆえ y_1 と z_1 はxの巾であるyとzと交換可能であ

る. $yz=x=y_1z_1$ より $w=y_1^{-1}y=z_1z^{-1}$, しかし y と y_1 は位数 m の交換可能な元かつ z と z_1 は位数 n の交換可能な元である. ゆえに $w^m=1$ かつ $w^n=1$, しかるに $(m,n)=1$ より $w=1$ となる. したがって $y_1=y$, $z_1=z$ となって表現の一意性は証明された.

この補題を繰り返して使用することによって次の補題が得られる.

補題 3.2.2. x が位数 $n=n_1n_2\cdots n_r$ の元で, $i\neq j$ に対して $(n_i,n_j)=1$ とする. すると, x は $x=x_1x_2\cdots x_r$, $x_ix_j=x_jx_i$, x_i の位数は n_i, と一意的に表わすことができる. すべての x_i は x の巾である.

特に, $n=p_1^{e_1}\cdots p_r^{e_r}$, $p_1,\cdots,p_r$ は互いに異なる素数とすると $n_i=p_i^{e_i}$ に対して上の結果を適用できる.

周期的アーベル群 A において, 位数が決められた素数 p の巾になる元の集合 P を考えよう. 単位元も, $p^0=1$ より含むものとする. $x^{p^a}=1$, $y^{p^b}=1$ とすると, $(xy)^{p^c}=1$, $c=\max(a,b)$ そして $(x^{-1})^{p^a}=1$. したがって P は部分群をなすがこれを **Sylow *p*-部分群**とよび $S(p)$ とかく. P を**アーベル *p*-群**とよぶ.

定理 3.2.3. 周期的アーベル群はその Sylow 部分群 $S(p)$ の直積である.

証：明らかに A の Sylow 部分群の直積 $\prod_p S(p)$ は A の部分群である. しかし補題 3.2.2 より $x\in A$ が位数 $n=p_1^{e_1}\cdots p_r^{e_r}$ ならば $x=x_1\cdots x_r$, $x_i\in S(p_i)$ となるから A のすべての元 x は Sylow 部分群の直積に含まれる. したがってこの直積は群全体 A に等しくなければならない.

3.3. 有限アーベル群. 不変数

当然のことではあるが, 有限アーベル群は周期的かつ有限生成である. 先の節の結果を適用すれば次の定理が成立する.

定理 3.3.1. 位数 $n=p_1^{e_1}\cdots p_r^{e_r}$ の有限アーベル群はシロー部分群 $S(p_1)$, $\cdots$, $S(p_r)$ の直積である. ここで $S(p_i)$ は位数 $p_i^{e_i}$ で位数 $p_i^{e_{i1}},\cdots,p_i^{e_{is}}$ の巡

回群の直積である．ただし $e_{i_1}+\cdots+e_{is}=e_i$ である．

証：位数 n のアーベル群においては元の位数は n の約数であるから，n を割らない素数に対する Sylow 部分群は単位群である．したがって $p_1, \cdots, p_r$ が n を割る相異なる素数ならばその群は直積 $S(p_1)\times\cdots\times S(p_r)$ である．しかし $S(p_i)$ の位数が分からない．あるものは単位群になるかもしれない．ところが $S(p_i)$ は単位群または位数 $p_i{}^{e_{i_1}}, \cdots, p_i{}^{e_{is}}$，の巡回群の直積であるから $S(p_i)$ の位数はこれらの位数の積 $p_i{}^{t_i}, t_i=e_{i1}+\cdots+e_{is}$ である．そして群全体の位数は $S(p_i)$ の位数の積となる．しかし整数 n の素因数分解の一意性によって，$p_i{}^{t_i}=p_i{}^{e_i}$ となる．この結果および定理 3.3.1 の結果として次の系が得られる．

系 3.3.1. 位数 n のアーベル群は p が n を割る素数ならば位数 p の元を含む．

有限アーベル p-群，$A(p)$ は，巡回群の直積として種々の方法で書くことができる．たとえば，$a^8=1$，$b^4=1$ ならば $A(2)=\{a\}\times\{b\}$ は位数 32 である．$c=ab$, $d=a^4b$ と置けば $c^8=1$，$d^4=1$，$a=c^5d^{-1}$，$b=c^4d$．そして $A(2)=\{c\}\times\{d\}$ となることはすぐ分かる．この場合 $A(2)$ は 2 通りの異なる方法で巡回群の直積となるが，因子の数とそれらの位数は等しい．一般にこのことはアーベル p-群に対しては正しいが，位数 6 の巡回群は位数 2 と 3 の巡回群の直積となるから，p-群でない有限アーベル群に対しては正しくない．A がアーベル群で位数 $p^{e_1}, \cdots, p^{e_r}$ の巡回群の直積となるとき $p^{e_1}, \cdots, p^{e_r}$ をこの群の**不変数**とよぶ．特に重要なのは，不変数が $p, \cdots, p$ の場合で，このとき A は**基本アーベル群**とよばれる．明らかにアーベル群 A の不変数は同型を除いて A を決定するが次の定理によって正確に与えられるように，これらは強い意味での不変数である．

定理 3.3.2. 有限アーベル p-群 A が 2 通りの方法，$A=A_1\times\cdots\times A_r=B_1\times\cdots\times B_s$，で巡回群の直積で表わせるならば，いずれの場合にも因子の数は等しく，$r=s$，そして $A_1, \cdots, A_r$ の位数は適当に並び換えることによって，$B_1, \cdots,$

B_s の位数に等しい．

証：Aが位数pのときはこの定理は明らかに成立するから，Aの位数に関する帰納法によって証明する．

Aを任意のアーベル p-群とするとき，$x^p=1$ となる元xからなる部分群をA_p, $y\in A$ に対して y^p の形の元からなる部分群を A^p，としよう．Aは基底 $a_1, \cdots, a_r, a_i$ の位数 $p^{e_i}, i=1, \cdots, r$ を持つ．$e_1\geqq e_2\geqq\cdots\geqq e_r$ となるように a_i をならべておく．すると A_p の基底は $a_1{}^{p^{e_1-1}}, \cdots, a_r{}^{p^{e_r-1}}$，かつ位数 p^r となることは容易に分かる．Aが基本アーベル群であれば $A^p=1$．さもなければ e_m を1より大の最初の巾とする．すなわち $e_1\geqq\cdots\geqq e_m>e_{m+1}=\cdots=e_r=1$．すると A^p は基底 $a_1{}^p, \cdots, a^p{}_m$ を持つ．

Aが第2の基底，$b_1, \cdots, b_s, b_i$ の位数 $p^{f_i}, i=1, \cdots, s, f_1\geqq f_2\geqq\cdots\geqq f_s$ を持つとしよう．すると，基底 $a_1, \cdots, a_r$ より A_p は位数 p^r そして基底 $b_1, \cdots, b_s$ より A_p は位数 p^s となる．したがって $r=s$．Aが基本アーベル群ならばこれで証明が完了したことになる．そうでなければ，$f_1\geqq f_2\geqq\cdots\geqq f_n>f_{n+1}=\cdots=f_s=1$ としよう．このとき A^p は不変数 $p^{e_1-1}, \cdots, p^{e_m-1}$ を持つ．さらに不変数 $p^{f_1-1}, \cdots, p^{f_n-1}$ を持つ．帰納法によって $m=n$ そして $e_1-1=f_1-1, \cdots, e_m-1=f_m-1$．$s=r$ を考慮すれば $e_1=f_1, \cdots, e_r=f_r$．ゆえに証明された．

系 3.3.2. 2個のアーベル p-群が同じ不変数を持たなければ，これらは同型でない．

定理 3.3.3. 不変数 $p^{e_1}, \cdots, p^{e_r}$, $e_1\geqq\cdots\geqq e_r$，を持つアーベル群Aが不変数 $p^{k_1}, \cdots, p^{k_t}$, $k_1\geqq\cdots\geqq k_t$ なる部分群Kを持つための必要十分条件は $t\leq r$ かつ $k_1\leq e_1, \cdots, k_t\leq e_t$ となることである．

証：まず始めにAの部分群Kの不変数の巾が定理の不等式を満たすことをAの位数に関する帰納法で証明する．Aの位数がpのときは明らかである．

K_p は A_p の部分群であるから，$t\leq r$，したがってAが基本アーベル群のときは証明された．$e_1\geqq\cdots\geqq e_m>e_{m+1}=\cdots=e_r=1$，かつ $k_1\geqq\cdots\geqq k_u>k_{u+1}=\cdots$

$=k_t=1$ とする．K^p は A^p の部分群で K^p と A^p の不変数はそれぞれ $p^{k_1-1}, \cdots, p^{k_u-1}$, および $p^{e_1-1}, \cdots, p^{e_m-1}$ となる．帰納法によって $u \leqq m$, $k_i-1 \leqq e_i-1, i=1, \cdots, u$. したがって $k_i \leqq e_i$, $i=1, \cdots, u$. また $k_{u+1}=\cdots=k_t=1$, $k_i \leqq e_i$, $i=u+1, \cdots, t$. ゆえに $k_i \leqq e_i$, $i=1, \cdots, t$.

定理の不等式が成立すれば与えられた不変数を持つAの部分群が一つ存在する．それを，Aの始めの t 個の基底の元の適当な巾に対する基底として選ぶことができる．しかし，与えられた群Aと部分群Kがあるとき，Kの基底がAの基底の元の巾からなるようにAの基底とKの基底を選ぶことができるというのは一般に正しくない．（演習問題．5．参照）

演 習 問 題

1. $a^3b^9c^9=1$, $a^9b^{-3}c^9=1$ を満たす元 a, b, c によって生成されたアーベル群Aがある．Aの基底と，その元の位数を求めよ．
2. 有限アーベル p-群は最高位数の元によって生成されることを証明せよ．
3. 不変数 p^3, p^2 を持つアーベル群は位数 p^2 の部分群をいくつ持つか．
4. 位数 p の部分群をちょうど p^2+p+1 個持つアーベル p 群の例を二つ示せ．
5. $a^{p^3}=1, b^p=1$ を満たす元 a, b によって生成されたアーベル群をAとする．Kを元 $x=a^pb$ で生成された部分群とする．Kの基底がAの基底の元の巾となるようにAおよびKの基底が選べないことを示せ．

第4章　Sylow の定理

4.1. Lagrange の定理の逆の不成立

Lagrange の定理によれば有限群の部分群の位数はその群の位数の約数である．しかし逆に，位数 n の群は m が n の対数のとき，位数 m の部分群を持つとは限らない．特に位数 12 の次の置換群[1] は位数 6 の部分群を持たない：

$$\begin{pmatrix}1,2,3,4\\1,2,3,4\end{pmatrix} \qquad \begin{pmatrix}1,2,3,4\\1,3,4,2\end{pmatrix}$$

$$\begin{pmatrix}1,2,3,4\\2,1,4,3\end{pmatrix} \qquad \begin{pmatrix}1,2,3,4\\1,4,2,3\end{pmatrix}$$

$$\begin{pmatrix}1,2,3,4\\3,4,1,2\end{pmatrix} \qquad \begin{pmatrix}1,2,3,4\\3,2,4,1\end{pmatrix}$$

$$\begin{pmatrix}1,2,3,4\\4,3,2,1\end{pmatrix} \qquad \begin{pmatrix}1,2,3,4\\4,2,1,3\end{pmatrix}$$

$$\begin{pmatrix}1,2,3,4\\2,3,1,4\end{pmatrix} \qquad \begin{pmatrix}1,2,3,4\\2,4,3,1\end{pmatrix}$$

$$\begin{pmatrix}1,2,3,4\\3,1,2,4\end{pmatrix} \qquad \begin{pmatrix}1,2,3,4\\4,1,3,2\end{pmatrix}$$

しかし，位数 2, 3, 4 の部分群は存在する．

したがって一般に，m が n を割るとき位数 n の群が位数 m の部分群を含むことは正しくない．しかし，もし，m が素数または素数巾のときは，そのような部分群が存在することは正しい．存在性と，そのような部分群の個数は次の **Sylow の定理**より分かる．Sylow の定理の出発点となる定理からはじめよう．

定理 4.1.1. 群 G の位数が素数 p で割れるならば G は位数 p の元を含む．

証：$n=mp$ を G の位数とする．$m=1$ ならば G は位数 p の巡回群となるか

1) この群を 4 次交代群とよぶ．(p. 65 参照)

ら定理は正しい．mに関する帰納法で証明する．Gが真の部分群Hで$(G:H)$がpで割れないものを含めば，Hの位数はpで割れるから帰納法の仮定よりHの位数pの元を含む．さて，Gのすべての真の部分群がpで割れる指数を持つと仮定しよう．1.6 より $n=n_1+n_2+\cdots+n_s$, n_i はGの元の共役類の元の数である．各 $n_i\neq 1$ はGの真の部分群の指数である．したがって，仮定よりpで割れる．$n_1=1$ とする．$n_i=1$ となるものの数はpの倍数である．元 a_i が共役類をなす必要十分条件は，a_i がGの中心Zにはいることである．ゆえに中心Zの位数はpで割れる．$z\in Z$ と任意の $g\in G$ に対して $zg=gz$，したがって特にZはアーベル群となる．定理 3.3.1 の系よりZは位数pの元を含む．

4.2. Sylow の定理

定理 4.1.1 よりpがGの位数を割る素数のとき，少なくとも一つの位数pの元が存在することが分かった．Gの位数が $n=p^m s$ ならば位数 $p^2, p^3, \cdots, p^m$ の部分群が存在することを示そう．

定理 4.2.1（第1 Sylow の定理）． Gの位数が $n=p^m s$, $p\nmid s$, p：素数，ならばGは位数 $p^i, i=1,\cdots,m$ の部分群を含む．そして位数 p^i, $i=1,\cdots,m-1$, の各部分群は少なくとも一つの位数 p^{i+1} の部分群の正規部分群である[1]．

証： i に関する帰納法で証明する．さきに述べたようにGは位数pの部分群を含む．Pを位数 $p^i, i\geq 1$ の部分群とする．GをPの両側剰余類でかく．$G=P+Px_2P+\cdots+Px_rP$, Px_jP におけるPの右剰余類の個数を a_j とする．$(G:P)=a_1+a_2+\cdots+a_r$, $a_j=(x_j^{-1}Px_j : x_j^{-1}Px_j\cap P)$, 両側剰余類 $P\cdot 1\cdot P=P$ に対して $a_1=1$ である．$a_j=1$ またはpの巾である．$p|(G:P)$ だから，1に等しい a_j の個数はpの倍数である．$a_j=1$ ならば $x_j^{-1}Px_j=P$ そして x_j と剰余類 $Px_j=x_jP$ はPの正規化群Kに属さねばならない．逆に $x_j\in K$ ならば $x_j^{-1}Px_j=P$ かつ $a_j=1$．したがって，$(K:P)$ は $a_j=1$ となる a_j の個数に等しいから $p|(K:P)$．ゆえに商群 K/P はpで割れる位数$(K:P)$

---

1) 換言すれば，P, Q をp-群かつ $P\supset Q$ とすると，$N_P(Q)\supset Q$ となる．

を持つ．K/P は位数 p の部分群 J^* を含む．定理 2.3.4 より $J^*=J/P$，$J \subseteq K$，$(J:P)=(J^*:1)=p$，となるから，J は P を含む位数 p^{i+1} の部分群である．そして P を正規部分群として含む．

定　義：群 P は単位元以外のすべての元の位数が素数 p の巾のとき p-群とよばれる．

定　義：群 G の部分群 S はそれが p-群であって G の部分群でより大きな p-群に含まれないとき Sylow 部分群[1]とよばれる．

これらの定義を用いて第1 Sylow の定理からの系を述べよう．

系 4.2.1. 位数 $n=p^m s$, $p \nmid s$, p：素数の有限群 G は位数 p^m の Sylow 部分群を含む．そして，すべての p-群で G の部分群であるものは G の一つの Sylow 部分群に含まれる．

位数 p^m のすべての群は p-群である．定理 4.1.1 よりもし群の位数が二つの異なる素数で割れれば，それは p-群ではない．したがってすべての有限 p-群の位数は p の巾，すなわち p^m，である．

系 4.2.2. 位数 p^m の p-群 P のすべての部分群は位数 p^{m-1} の極大部分群に含まれる．P のすべての極大部分群は正規部分群である．

定理 4.2.2（第2 Sylow の定理）. 有限群 G において Sylow p-部分群は共役である．

証：P_1 と P_2 を二つの Sylow p-部分群とする．すると，$G=P_1P_2+P_1x_2P_2+\cdots+P_1x_sP_2$，$P_1x_iP_2$ における P_2 の右剰余類の数を b_i とする．$b_i=(x_i^{-1}P_1x_i : x_i^{-1}P_1x_i \cap P_2)$ そして b_i は 1 または p の巾である．しかし，$b_1+\cdots+b_s=(G:P_2)$ は p の巾ではない．ゆえにある i が存在して，$b_i=1$ となるから $x_i^{-1}P_1x_i=P_2$.

---

1) Sylow p-部分群または p-Sylow 群ともよばれる．そして素数 p があきらかな場合は p を省略して単に Sylow 部分群とよぶ．

定理 4.2.3 (第3 Sylow の定理). 有限群Gの Sylow p-部分群の数は $1+kp$ の形で，Gの位数の約数である．

証：ただ一つの Sylow p-部分群が存在するときは明らかである．$S_0, S_1, \cdots, S_r$ を Sylow p-部分群とする．S_0 の元で変換すればこれらは共通部分のない，いくつかの共役集合に分かれる．第2 Sylow の定理より S_i はその正規化群 K_i の中でただ一つの Sylow 部分群である．したがって，S_0 における $S_i(i\neq 0)$ の正規化群は，S_0 の真の部分群であり，S_0 による S_i の共役部分群の数は p の巾，$p^e, e\geq 1$ である．ゆえに，$r=p^{e_1}+\cdots+p^{e_s}=kp$，そして $1+r=1+kp$ 個のGの Sylow p-部分群が存在する．Sylow p-部分群の数は第2 Sylow の定理によって S_0 の正規化群の指数に等しい．ゆえに，Gの位数の約数である．

定理 4.2.4. 有限群Gにおいて，Kを Sylow p-部分群Pの正規化群とする．Hを$G\supseteq H\supseteq K\supseteq P$ となるGの任意の部分群とすればHはG中Hの正規化群に等しい．

証：$x^{-1}Hx=H$ と仮定する．すると $H\supseteq x^{-1}Px=P'$ はHの Sylow p-部分群である．したがってある元 $u\in H$，が存在して $u^{-1}P'u=P$，より $u^{-1}x^{-1}Pxu=P$，かつ $xu\in K$．ゆえに，$x\in H$ となって，HはHの正規化群に等しい．

次の定理は，この定理自身も興味があるが，後の章で述べるように重要な応用がある．

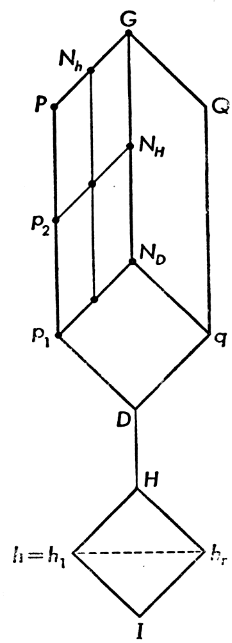


図 2. Burnside の定理

定理 4.2.5 (Burnside). 有限群Gにおいて p-群 hが一つの Sylow p-部分群中正規であるが，それを含むある他の Sylow 部分群中で正規でないとすれば，r 個の共役な群，$h=h_1, h_2, \cdots, h_r$ が存在して，いずれ

も $H=h_1\cup h_2\cup\cdots\cup h_r$ 中正規であるが，どの Sylow p-部分群においてもすべてが正規となることはない．ただし，$r>1$，$r\not\equiv 0 \pmod{p}$ となる．$h_1, \cdots, h_r$ はHの正規化群 N_H における h と共役な群の全集合をなす．

証：N_h を h の正規化群とする．QをGの Sylow p-部分群でhを含みhがQ中正規でなくかつ $D=N_h\cap Q$ が極大とする．q をDのQにおける正規化群そしてN_D をDのGにおける正規化群とする．hはQのある部分群において正規かつ指数pであるが h は Q 中正規ではないから，$Q\supseteq q\supsetneq D\supset h$ となる[1]．$D=N_h\cap Q$だから，hはq中正規ではなく[2]，またN_D中正規ではない．$h=h_1, \cdots, h_s, s>1$ を N_Dにおける h と共役な部分群とする．hはD中正規でかつN_D はDに自己同型を引き起こすから，すべての h_i はD中正規である．特に，$H=h_1\cup h_2\cup\cdots\cup h_s\subseteq D$ において正規である．N_D の元はHをHに変換するからHの正規化群 N_H は N_D を含む．p_1 を $N_h\cap N_D$ の Sylow 部分群，そして$p_1\subseteq P_1$ をN_h の Sylow 部分群とする．仮定によって P_1 はGの Sylow 部分群である[3]．P_1 におけるDの正規化群はDに等しくないから$D\subset p_1, N_h\cap N_D\subseteq N_D\subseteq N_H$，そして $p_2\supseteq p_1$ を N_H の Sylow 部分群とする．さらに$P\supseteq p_2$ をGの Sylow 部分群とする．$P\nsubseteq N_h$ ならば $P\cap N_h\supseteq p_1\supset D$ となって，Dの極大性に矛盾する．したがって $P\subseteq N_h$．p_2 は N_H の Sylow 部分群であったから $N_h\cap N_H\supseteq P\cap N_H=p_2$.

$h=h_1, \cdots, h_s, \cdots, h_r$ を N_H における h の共役部分群とする．するとすべてHの正規部分群となる．h の N_H における正規化群は $N_H\cap N_h$ に等しく，それゆえ N_H における h の共役部分群の数は $r=(N_H : N_H\cap N_h)$：しかし，$N_H\cap N_h\supseteq p_2$ は N_H の Sylow 部分群であるから $r\not\equiv 0 \pmod{p}$.

すべての $h_1, \cdots, h_r$ がある Sylow 部分群 S_p の正規部分群ならば $S_p\subseteq N_H$ かつ N_H のすべての Sylow 部分群は h_i のすべてを含みかつ正規化する．し

---

1) 第1 Sylow の定理より $D\supset h$. $D=q$ とすると再び第1 Sylow の定理より $Q=q=D$. したがってhはQ中正規となってQのえらび方に矛盾する．ゆえに $q\supset D\supset h$ となる．

2) hがq中正規とすると $N_h\supseteq q$ より $D=N_h\cap Q\supseteq q$ となって $q\supset D$ に矛盾する．

3) この定理の仮定よりhは一つの Sylow p-部分群中正規であるから，N_h の Sylow p-部分群はGの Sylow p-部分群である．

かし，$q \subseteq N_D \subseteq N_H$ は N_H の p-群で h_1 を正規化しない．

4.3. 有限 p-群

Sylow の定理より位数 $n=p_1^{e_1}\cdots p_r^{e_r}$ の群Gは各 i に対して，位数 $p_i^{e_i}$ の部分群を含み，この位数のすべての部分群は互いに共役なので同型である．したがって有限群を構成する問題は，次の２つの部分に分けて考えられる：1) 素数巾の位数の群の構成，2) n を割る素数巾の位数の群と位数 n の群との関係．すべての Sylow 部分群が巡回群ならば（たとえばすべての $e_i=1$ のとき），第２の問題は解決できる．結果は第９章定理 9.4.3 にある．これらの問題は一般には解決されないとはいえ，第２の問題に用いるために，第１の問題を解かねばならない．一つの群を形成するために Sylow 部分群を結合することの困難さは素数巾の位数の群すなわち p-群の複雑さに非常に基づいているように思われる．

さて，p-群の性質で非常に重要なのは次の定理である．

定理 4.3.1. 有限 p-群の中心な単位元以外の元を含む．

証：Pを有限 p-群とし，Pを共役類の和で表わす：

(4.3.1) $$P=C_1+G_2+\cdots+C_r$$

ここで C_1 は単位元だけの類とする．h_i を C_i の元の数とすれば定理 1.6.1 より，h_i はPの部分群の指数に等しいから，中心の元に対しては 1，他の元に対してはｐの巾となる．Pの位数を p^m とすれば

(4.3.2) $$p^m=h_1+h_2+\cdots+h_r$$

$h_1=1$ だから，(4.3.2) において残りすべての h_j が p の真の巾となることはない．したがって他の h_j で１となるものが存在する．ゆえにPの中心は単位元より大きい．

系 4.2.2 を定理として改めて述べよう．

定理 4.3.2. 位数 p^m の p-群Pのすべての真の部分群は位数 p^{m-1} の極大

部分群に含まれる．そしてPのすべての極大部分群は正規部分群である．

第1の Sylow の定理から，p-群のどんな真の部分群もその正規化群と一致することはないことが分かる．この事実の逆を次に述べよう．

定理 4.3.3. 有限群Gにおいてどんな真の部分群もその正規化群に等しくないための必要十分条件はGが Sylow 部分群の直積となっていることである[1]．

証：どんなGの真の部分群もその正規化群に等しくないと仮定する．定理 4.2.4 より Sylow 部分群Pの正規化群Kは群全体Gに一致する．したがってPはGの正規部分群である．定理 2.5.2 を考慮して，Sylow 部分群の和は Sylow 部分群の直積となる．ゆえにGは Sylow 部分群の直積である．$G=P_1\times\cdots\times P_r$, P_i は位数 $p_i^{e_i}$ の部分群，かつ $i\neq j$ に対して $p_i\neq p_j$ と仮定する．$g_i\in P_i$ に対して，$g=g_1g_2\cdots g_r$ とすれば補題 3.2.2 の条件が成立し，各 g_i は g の巾である．したがって一元 g がGの部分群Hにはいれば，その成分 g_i もHの元となるからHは P_i の部分群 $H_i=H\cap P_i$ の直積でなければならない．$H=H_1\times\cdots\times H_r$. HがGの真の部分群であれば，ある H_j が存在して H_j は P_j の真の部分群となる．この H_j を P_j のより大きな部分群でそれが正規となるもので置き換えれば，Hより大きな部分群で，Hが正規となるものが得られる．

定理 4.3.4. Aが p-群Pに含まれる位数pの正規部分群とすればAはPの中心にはいる．

証：Aは位数がpだから巡回群で一元aによって生成される．Aの元は $1, a,\cdots,a^{p-1}$ である．Aは正規部分群だからaの共役元は集合 $a, a^2,\cdots,a^{p-1}$ の中にはいる．aと共役な元の個数はその中心化群の指数に等しいから，1またはpの巾である．しかし，共役元の個数はたかだか $p-1$ 個であるから可能性は1のみである．ゆえにa，すなわちAはPの中心に含まれる．

---

[1] このような有限群を巾零群とよぶ（第10章参照）．

4.4. 位数 p, p^2, pq, p^3 の群

素数位数 p の群は真の部分群を持たないから単位元以外の任意の元で生成された巡回群である．定理 1.5.4 において，どんな真の部分群をも持たない群 G は素数位数の巡回群であることを示した．

位数 p^2 の群 G はもし巡回群でなければ2個の位数 p の異なる部分群 $\{a\}$ と $\{b\}$ を含む．$a^p=1$, $b^p=1$. そして $\{a\}\cap\{b\}=\{1\}$. 系 4.2.2 よりこれらはどちらも極大部分群であるから正規部分群である．したがって定理 3.2.1 より $G=\{a\}\times\{b\}$. すなわち G は基底 a, b, を持つアーベル群である．

G の位数が pq, p, q は素数で $p<q$ と仮定する．第3の Sylow の定理より位数 q の部分群の個数は $1+kq$ 個で p を割り切るから1に等しい．$k=0$. 位数 q の部分群がただ一つであるからそれは正規部分群である．$\{b\}$, $b^q=1$ とする．位数 p の部分群の個数は $1+kp$ 個で q を割り切るからそれは1または q である．個数を1個とすればある元 a に対して正規部分群 $\{a\}$, $a^p=1$ が存在し，G は $\{a\}$ と $\{b\}$ の直積となる．しかし，$c=ab$ は位数 pq だから G は巡回群である．位数 p の部分群 $\{a\}$ が $q=1+kp$ 個存在する場合を考える．$\{a\}$ は正規ではない．

$$a^p=1,\quad b^q=1,$$

$\{b\}$ は正規であるからある整数 r が存在して，$a^{-1}ba=b^r$. $r=1$ ならば G はアーベル群となって上に述べたように巡回群となる．$r\neq 1$ とする．任意の i に対して $a^{-1}b^ia=b^{ir}$, 特に $a^{-1}b^ra=b^{r^2}$, したがって $a^{-2}ba^2=a^{-1}b^ra=b^{r^2}$. もっと一般に，帰納法によって $a^{-j}ba^j=b^{r^j}$ となることが分かる．$j=p$ に対して $b=a^{-p}ba^p=b^{r^p}$. ゆえに，$r^p\equiv 1 \pmod{q}$. r に関するこの必要条件は十分条件にもなっていることは，任意の2元の積に対して

$$(a^ub^v)(a^xb^y)=a^{u+x}b^{vr^x+y}$$

となる一般的な法則と，この法則が位数 pq の群を定義することを証明することによって確かめられる．このことはもっと一般的な法則，定理 6.5.1 の特殊な場合である．

位数 p^3 の群に対しては，不変数が各々 (p^3), (p^2, p), (p, p, p) となる 3 種の型のアーベル群が存在する．非アーベル群を決めるために，$p=2$ と $p=$奇素数の場合を分けて考える．まず第一に $p=2$ として位数 8 の非アーベル群を考える．巡回群ではないから位数 8 の元は存在しない．すべての元の位数が 2 であれば，$(ab)^2=1$，すなわち $abab=1$，$ba=a^2bab^2=ab$ となって群はアーベル群となる．したがって位数 4 の元 a が存在しなければならない．$a^4=1$, $b\notin\{a\}=A$ ならば $G=A+Ab$ かつ $b^2\in A$．もし $b^2=a$ または a^3 とすれば b の位数は 8 となり G は巡回群となる．ゆえに $b^2=1$ または a^2 となる．A は正規部分群であるから $b^{-1}ab\in A$，そして $b^{-1}ab$ は位数 4 の元であるから $b^{-1}ab=a$ または a^3, $b^{-1}ab=a$ ならば G はアーベル群となる．したがって $b^{-1}ab=a^3$．ゆえに，2 個の非アーベル群が得られた．すなわち定義関係式

$$a^4=1,\quad b^2=1,\quad b^{-1}ab=a^3,$$

を満たす二面体群と

$$a^4=1,\quad b^2=a^2,\quad b^{-1}ab=a^3$$

を満たす四元数群である．これらの関係式が位数 8 の群を定義し，互いに同型でないことは容易に分かる[1]．

最後に，奇素数 p に対して，位数 p^3 の非アーベル群を決定する．G は巡回群でないから位数 p^3 の元は含まない．まず始めに G が位数 p^2 の元 a を含むと仮定しよう．$a^{p^2}=1$．すると $A=\{a\}$ は極大部分群だから正規である．$b\notin A$ とする．すると $G=A+Ab+\cdots+Ab^{p-1}$, $b^p\in A$, $b^{-1}ab=a^r$, G は非アーベル群だから $r\neq 1$．j に関する帰納法によって $b^{-j}ab^j=a^{r^j}$, b^p は A の元だから a とは可換である．ゆえに $a=b^{-p}ab^p=a^{r^p}$, $r^p\equiv 1 \pmod{p^2}$．Fermat の定理より $r^p\equiv r \pmod{p}$．したがって $r\equiv 1 \pmod{p}$．$r=1+sp$ とかく．$js\equiv 1 \pmod{p}$ より

$$b^{-j}ab^j=a^{(1+sp)j}=a^{1+sjp}=a^{1+p}$$

$(j, p)=1$, $b^j\notin A$ より b を b^j で置き換えても

1) 四元数群では位数 2 の元は a^2 だけであるが，二面体群では $\{a, b\}-\{a\}$ の元はすべて位数 2 である．すなわち位数 2 の元は 5 個存在する．

$$G=A+Ab+\cdots+Ab^{p-1}$$

ここで $b^{-1}ab=a^{1+p}$.

$b^p\in A$ より $b^p=a^t$, b の位数は p^3 ではないから，t は p の倍数でなければならない．$b^p=a^{up}$ とする．

$a^ib=ba^{i(1+p)}$ より

$$\begin{aligned}(ba^{-u})^p&=b^pa^{-u[1+(1+p)+(1+p)^2+\cdots+(1+p)^{p-1}]}\\&=b^pa^{-up-up(1+2+\cdots+p-1)}\\&=b^pa^{-up}=1\end{aligned}$$

p は奇数であるから $1+2+\cdots+p-1=p(p-1)/2$ は p の倍数である．$b_1=ba^{-u}$ とすれば，$a^{p^2}=1$, $b_1{}^p=1$, $b_1{}^{-1}ab_1=a^{1+p}$ が得られる．最後の式は $b_1{}^{-1}ab_1=a^u(b^{-1}ab)a^{-u}$ より出る．

最後の場合として，G が位数 p^2 の元を含まないと仮定する．中心 Z の位数が p^2 ならば G はアーベル群となるから，Z の位数は p である．G/Z は $x^p=1$, $y^p=1$, $yx=xy$ の形の群である．準同型 $G\to G/Z$ において，$a\to x$, $b\to y$ ならば $a^p=1$, $b^p=1$, $a^{-1}b^{-1}ab=c\in Z$. $a^{-1}b^{-1}ab=1$ ならば a, b, と Z は G を生成するから G はアーベル群になる．ゆえに c は Z の生成元で

$$a^p=1,\ b^p=1,\ c^p=1,\ ab=bac,\ ac=ca,\ bc=cb.$$

となる．

定義関係式の表 [1), 2)]

I. Gの位数 p

1) 巡回群．$a^p=1$.

II. Gの位数 p^2

1) 巡回群．$a^{p^2}=1$.

2) 基本アーベル群．$a^p=1$, $b^p=1$, $ba=ab$

---

1) 素数位数の群を除いて，有限単純群の位数は偶数であるから，必ず Sylow 2-部分群を含む．これらの位数 2, 2^2, 3^3 の群の中で有限単純群の Sylow 2-部分群となるものは，基本アーベル群および二面体群だけである．さらに二面体群を Sylow 2-部分群として持つ有限単純群は Gorenstein と Walter によって1960年代に完全に分類された．しかし基本アーベル群を Sylow 2-部分群として持つ有限単純群はまだ完全には分類されていない．

2) 奇素数 p に対して有限単純群の Sylow p-部分群に関する結果は何も得られていない．

III. Gの位数 pq, $p<q$

1) 巡回群. $a^{pq}=1$.

2) 非アーベル群. $a^p=1$, $b^q=1$, $a^{-1}ba=b^r$, $r^p\equiv 1 \pmod{q}$,

$r\not\equiv 1 \pmod{q}$, p は $q-1$ を割り切る.

$z^p\equiv 1 \pmod{q}$, $z\not\equiv 1 \pmod{q}$ の解は $r, r^2, \cdots, r^{p-1}$ で, $\{a\}$ の生成元として a を a^j で置き換えることは r を r^j で置き換えることであるから, 同じ群をつくる.

IV. Gの位数 p^3

アーベル群

1) $a^{p^3}=1$.

2) $a^{p^2}=1$, $b^p=1$, $ba=ab$.

3) $a^p=b^p=c^p=1$, $ba=ab$, $ca=ac$, $cb=bc$.

位数 $2^3=8$ の非アーベル群

4) 二面体群. $a^4=1$, $b^2=1$, $ba=a^{-1}b$.

5) 四元数群. $a^4=1$, $b^2=a^2$, $ba=a^{-1}b$.

位数 p^3, p 奇素数の非アーベル群

4) $a^{p^2}=1$, $b^p=1$, $b^{-1}ab=a^{1+p}$.

5) $a^p=1$, $b^p=1$, $c^p=1$, $ab=bac$, $ca=ac$, $cb=bc$.

演 習 問 題

1. Hを有限群Gの正規部分群, かつ $(G:H)$ が p と素ならば, HはGのすべての Sylow p-部分群を含むことを証明せよ.
2. 群Gにおいて, 位数 p^a の正規部分群KはGのすべての Sylow p-部分群に含まれることを証明せよ.
3. p, q を相異なる素数とするとき, 位数 p^2q の群は正規な Sylow 部分群を含むことを証明せよ.
4. 位数 200 の群は正規な Sylow 部分群を含むことを証明せよ.
5. 正規部分群を含まない位数 168 の群には位数 7 の元が何個存在するか.
6. 次の表は 1 から 20 までの各位数の相異なる群の個数の表である. 16 以外のすべての位数に対して, この表を確認せよ.

位数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
個数	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1	5	1	5

第5章 置　換　群

5.1. 巡　環[1)]

第1章の Caley の定理で，すべての群は置換群として表わせることを述べた．そこで述べたように，一つの群は種々の方法で置換群として表わせる．置換 π に対して，π が x_i を x_j にうごかすことを $(x_i)\pi=x_j$ とかくことにする．

有限巡環とは，有限個の文字の集合 $x_1, x_2, \cdots, x_n$ の上の置換 π であって，$(x_1)\pi=x_2, \cdots, (x_{n-1})\pi=x_n, (x_n)\pi=x_1$ となるものである．

無限巡環とは，無限個の文字の集合 $x_i, i=-\infty, \cdots, +\infty$ 上の置換 π であって，$(x_i)\pi=x_{i+1}, i=-\infty, \cdots, +\infty$ となるものである．

我々は，有限巡環を $(x_1, x_2, \cdots, x_n)$ で表わし，無限巡環を $(\cdots, x_{-1}, x_0, x_1, \cdots)$ で表わす．巡環 $(x_2, \cdots, x_n, x_1)$ は $(x_1, x_2, \cdots, x_n)$ と同じ置換を表わすことは明らかである．

定理 5.1.1. 文字の集合 S の上の任意の置換 π が与えられたとする．すると S は，共通部分のない部分集合で，π が各部分集合上の巡環を表わすように分解される．

証：x_1 を S の任意の文字とする．$(x_1)\pi=x_1$ ならば，(x_1) はそれ自身で一つの巡環となる．$(x_1)\pi\neq x_1$ ならば，$(x_1)\pi=x_2$ とかく．$(x_2)\pi=x_3, \cdots, (x_i)\pi=x_{i+1}$ とかき文字が重複しないならばこの操作を限りなくつづける．$(x_1)\pi=x_2, \cdots, (x_{n-1})\pi=x_n$ はすべて相異なるが，$(x_n)\pi$ がすでに用いた文字になると仮定する．すなわちある $i=1, \cdots, n$ が存在して $(x_n)\pi=x_i$．$i=2, \cdots, n$ ならば，$(x_{i-1})\pi=x_i$ となって，仮定 $x_n\neq x_{i-1}$ に矛盾する．したがって $(x_n)\pi=x_1$ となり，π の文字 $x_1, \cdots, x_n$ の上への作用として，有限巡環 $(x_1, \cdots, x_n)$

---

1) 巡回置換ともいう．

が得られた．$(x_1)\pi^i=x_{i+1}$ がすべての相異なる $i=1,\cdots,$ に対して成立すれば，x_0 を $(x_0)\pi=x_1$ となる文字とする．$(x_{i-1})\pi=x_i$，$i=0,-1,-2,\cdots,$ によって連続的に，$x_{-1},x_{-2},\cdots,$ を定義する．π は相異なる2文字を同じ文字に移さないから，これらはすべて相異なる．このようにSの各元は，π によって一つの巡環の中で置換される文字の集合の一部である．$(x)\pi=y$ において，x または y のどちらかが他の文字を一意的に決定するから，任意の文字が巡環全体を決定することは明らかである．したがって異なる巡環は共通な文字を有しない．

我々は置換 π を巡環の積で書くことができ，そしてその各巡環は共通な文字を含まないから巡環の並ぶ順序は問題ではない．長さ1の巡環は，省略される習慣がある．すなわち，省略されたすべての文字は，固定されるものと考える．

したがって $\pi=(1)(2)(3,4,5)=(3,4,5)$．この規約によって，巡環の数が有限のときはいつでも，置換はその各巡環のなす群の積と考えられる．

定理 5.1.2. 置換 π の位数は，その巡環の長さの最小公倍数に等しい．

証：巡環 $(x_1,\cdots,x_n)$, $(x_i)\pi^j=x_{i+j}$ において，$i+j$ は n を法として還元される．したがって，$(x_i)\pi^t=x_i$ となる必要十分条件は，t が n の倍数となることである．それゆえ $(x_i)\pi^m=x_i$ が，すべての $x_i\in S$ に対して成立する必要十分条件は，m が π のすべての巡環の長さの倍数となることである．ここでは $\pi^m=1$．π が長さ無限の巡環を含めば，π は無限位数である．

次の補題は，計算上有効である．

補題 5.1.1.

$$T=(a_{11}\cdots a_{1r})(a_{21}\cdots a_{2s})\cdots(a_{m1}\cdots a_{mt})$$

かつ，

$$S=\begin{pmatrix}a_{11}\cdots a_{1r}a_{21}\cdots a_{2s}\cdots a_{m1}\cdots a_{mt}\\ b_{11}\cdots b_{1r}b_{21}\cdots b_{2s}\cdots b_{m1}\cdots b_{mt}\end{pmatrix}$$

ならば，

$$S^{-1}TS=(b_{11}\cdots b_{1r})(b_{21}\cdots b_{2s})\cdots(b_{m1}\cdots b_{mt}).$$

特別な元 b_{jk} に対して，

$$b_{j,k}\xrightarrow{S^{-1}}a_{j,k}\xrightarrow{T}a_{j,k+1}\xrightarrow{S}b_{j,k+1}$$

したがって $S^{-1}TS$ によって，$b_{jk} \to b_{j,k+1}$ となる．

文字の集合の上のすべての置換のなす群を**対称群**（symmetric group）とよぶ．n 文字上の対称群は，しばしば S_n で表わされる．

定理 5.1.3. 2個の置換が対称群において共役であるための必要十分条件は各長さの巡環を同じ個数だけ持つことである．

証：必要性は上の規則からわかる．十分性に対しては，

$$T=(a_{11}\cdots a_{1r})(a_{21}\cdots a_{2s})(a_{m1}\cdots a_{mt})$$
$$R=(b_{11}\cdots b_{1r})(b_{21}\cdots b_{2s})(b_{m1}\cdots b_{mt})$$

と仮定する．ただし長さ1の巡環をも含んでいるものとする．仮定より，TとRは各長さの巡環を同じ個数だけ含むから，巡環は上に書いたように番号付けられていると仮定して差し支えない．

$$Q=\begin{pmatrix}a_{11}\cdots a_{1r}\cdots a_{m1}\cdots a_{mt}\\ b_{11}\cdots b_{1r}\cdots b_{m1}\cdots b_{mt}\end{pmatrix}$$

とすれば，$Q^{-1}TQ=R$．この定理は有限性の条件を必要としないし，“同じ個数”とは含まれる濃度が同じことを意味していることに注意しよう．含まれる文字の個数が無限ならば，TとRは長さが1より大の巡環を同じ個数だけ含みしかも異なる個数の文字を固定するかもしれないから，長さ1の巡環を含めなければならない．したがって，$T=(0,1)(2,3)(4,5)\cdots$ と $R=(0)(1,2)(3,4)(5,6)\cdots$ は，文字 $0,1,2,3,\cdots$ 上の対称群において共役でない．

5.2. 可 移 性

定理 5.2.1. Gを文字 $x_1,\cdots,x_n$ 上の置換群とする．Sをこれらの文字の任意の部分集合とする．すると，Gの置換でSのすべての文字を固定するものは，部分群Kを形成する．Sの文字をSの文字の上に移す置換は，部分群Hを形成し，Kを正規部分群として含む．

証：2元 a,b がSの文字をSの文字に移すか，または，Sの文字を固定す

れば，ab と a^{-1} も同様である．ゆえに，定理で述べた部分群 H と K が存在する．$h\in H$, $k\in K$ とすれば，$h^{-1}kh$ は S の元を固定するから，K は H の正規部分群である．

定　義：文字 $x_1, \cdots, x_n$ 上の置換群を G, そして，$x_1, \cdots, x_n$ の部分集合を S とする．このとき，すべての $\sigma\in G$, $x_i\in S$ に対して，$(x_i)\sigma\in S$, かつ $x_i, x_j \in S$ に対して，$\sigma\in G$ が存在して，$(x_i)\sigma=x_j$ が成り立つとき，G は S 上**可移的**（transitive）であるとよばれる．S の文字は，**可移域**とよばれる．

定理 5.2.2. 固定された文字 x_1 に対して集合 S が $x_i=(x_1)\sigma$, $\sigma\in G$ となるすべての x_i からなるとき，S は可移域である．

証：$(x_1)\sigma=x_i$, $(x_1)\tau=x_j$ とすれば，$(x_i)\sigma^{-1}\tau=x_j$. さらに，$(x_1)\sigma=x_i$, $(x_i)\rho=x_k$ ならば，$(x_1)\sigma\rho=x_k$.

定理 5.2.3. 置換群 G に対して S が可移域で x_1 が S の文字であれば各 $x_i\in S$ に対して，$\sigma_i\in G$ で $(x_1)\sigma_i=x_i$ となるものを選べる．H を G の部分群で，x_1 を固定するものとする．すると $G=H\sigma_1+\cdots+H\sigma_i+\cdots$.

証：$h\in H$ に対して，$g=h\sigma_i$ とすれば $(x_1)g=x_i$, したがって剰余類 $H\sigma_i$ は相異なる．さらに，g を G の任意の元とする．すると $x_i\in S$ が存在して，$(x_1)g=x_i$. ゆえに，$(x_1)g\sigma_i^{-1}=x_1$ より，$g\sigma_i^{-1}\in H$, $g=h\sigma_i\in H\sigma_i$, すなわち剰余類 $H\sigma_i$ は G をうめる．

系 5.2.1. S を r 個の文字からなる G の可移域とする．すると，S の一文字を固定する部分群 H は，G 中指数 r である．

定　義：群 G は S 上可移的で，S の任意の順序づけられた k 個の相異なる文字が G のある元で S の任意の順序づけられた k 個の相異なる文字の上に置換されるとき，**k-重可移**（k-ply transitive）と呼ばれる．

定理 5.2.2 の類似が，k-重可移群に対して成立する．G が k 個の文字 x_1,

$x_2, \cdots, x_k$ を他の順序づけられたSの文字 $y_1, y_2, \cdots, y_k$ に移すならば，GはSの文字上 k-重可移である．またGの部分群でSの $r<k$ 個の文字を固定するものは，Sの残りの文字上 $(k-r)$-重可移である．またGが r-重可移で，r 個の文字を固定する部分群Hが s-重可移ならば，Gは $(r+s)$-重可移である．

5.3. 置換による群の表現

抽象群はいくつかの方法で置換群として表現されることはすでに注意した．置換の群Pは，もし群GからPの上への写像，$g \to \pi(g)$, $g \in G$, $\pi(g) \in P$ が存在して，$\pi(g_1)\pi(g_2) = \pi(g_1 g_2)$ となるときGの表現と呼ばれる．Pは必然的にGの準同型像となることに注意する．PがGと同型になるとき，PをGの**忠実**（faithful）な表現という．Gのすべての準同型像はGの正規部分群による商群によって与えられるので，Gのすべての可移置換表現は部分群の左剰余類上で得られる．

位数６の非アーベル群は，３文字そしてまた６文字上の可移置換群として忠実に表現されるから，抽象群として同型な群を置換群としては区別しなければならない．

定　義：集合 S_1 上の置換群 P_1 と集合 S_2 上の置換群 P_2 は，P_1 と P_2 の間の同型写像 $\pi_{P_1} \leftrightarrows \pi_{P_2}$ および S_1 と S_2 の間の１対１の対応 $x_i \leftrightarrows y_i$ が存在して，$(x_i)\pi_{P_1} = x_j$ となる必要十分条件が，$(y_i)\pi_{P_2} = y_j$ となるとき，置換群として同型であるという．

定理 5.3.1. 群Gおよび部分群Hがある．

a）各 $g \in G$ に対して，Hの左剰余類の集合上の置換

$$\pi(g) = \begin{pmatrix} Hx \\ Hxg \end{pmatrix}, \quad x \in G$$

が存在する．

b）$g \to \pi(g)$ は，Hの相異なる左剰余類の集合上の可移置換群としてのG

の表現である．$\pi(g)$ がHを固定する必要十分条件は，$g \in H$ となることである．

逆に，$g \to \pi(g)$ が集合S上の可移置換群PとしてのGの表現と仮定する．

c）Sの一元を s_1 とする．$\pi(g)$ が s_1 を固定するような g の全体は，Gの部分群Hとなる．

d）Sの元はHの左剰余類と1対1の対応がつく．それゆえ，Pは a）と b）において与えられた置換 $\pi(g)$ のなす群と，置換群として同型になる．

証：a）$Hx \to (Hx)g = Hxg$ は，各左剰余類 Hx を一意的に定まる左剰余類 Hxg の上に写像する．$(Hxg^{-1})g = Hx$ より，$\pi(g) = \begin{pmatrix} Hx \\ Hxg \end{pmatrix}$ は，相異なるHの左剰余類の集合上の置換である．

b）$(Hxg_1)g_2 = Hx(g_1g_2)$ より $\pi(g_1)\pi(g_2) = \pi(g_1g_2)$，したがって，$g \to \pi(g)$ はGの表現である．$H \to Hg = H$ となる必要十分条件は，$g \in H$ である．換言すれば，$\pi(g)$ がHを固定する必要十分条件は，$g \in H$ である．$\pi(x)$ によって $H \to Hx$ となるから，表現は可移である．

c）$(s_1)\pi(g_1) = s_1$，$(s_1)\pi(g_2) = s_1$ ならば，$(s_1)\pi(g_1g_2) = s_1$ かつ $(s_1)\pi(g_1{}^{-1}) = s_1$ となるから，部分群Hをなす．

d）Pは可移的であるから，$(s_1)\pi(g) = s_i$ となる g は存在する．このような g の一つを x_i で表わせば，この集合は左剰余類 Hx_i となる．ここでHは s_1 を固定する c）における部分群である．逆に左剰余類 Hx のすべての元は対応する置換が s_1 を同じ像の上に写像するという性質を持つ．これによって，S の元とHの左剰余類との間に1対1の対応 $s_i \leftrightarrows Hx_i$ が得られた．P_1 をHの左剰余類の集合上の置換群で，$g \in G$，$\pi_1(g) = \begin{pmatrix} Hx \\ Hxg \end{pmatrix}$ によって，a)，b）で与えられたものとする．Pにおいて $(s_i)\pi(g) = s_j$ ならば，$(s_1)[\pi(x_i)\pi(g)] = s_j$ となるから，$x_ig \in Hx_j$ したがって $(Hx_i)g = Hx_j$；逆にこの関係式より $(s_i)\pi(g) = s_j$．それゆえ，$s_i\pi(g) = s_j$ となるための必要十分条件は，$Hx_i\pi_1(g) = Hx_j$ である．とくに $\pi(g)$ が単位元であるための必要十分条件は，$\pi_1(g)$ が単位元となることである．したがって P と P_1 はGの準同型像で，どちらも同

じ核をもち，$\pi(g)\leftrightarrows\pi_1(g)$ は P と P_1 の間の同型である．S と H の左剰余類の集合の間の１対１の対応 $s_i\leftrightarrows Hx_i$ によって，P は置換群として P_1 と同型になる．その理由は，$(s_i)\pi(g)=s_j$ となる必要十分条件は，$Hx_i\pi_1(g)=Hx_j$ であるからである．

この定理によって，我々は群 G の任意の可移置換表現を部分群 H の上の表現として述べることができる．もし H が単位群であれば，この表現は 1.4 において述べたように右正則表現となる．

定理 5.3.2. 定理 5.3.1 の表現 $g\to\pi(g)$ において，単位元に写像される G の元は，H に含まれる G の最大正規部分群を形成する．それゆえ，この表現が忠実であるための必要十分条件は，H が単位群より大きな G の正規部分群を含まないことである．

証：どんな g に対して，$\pi(g)$ は単位元となるか．ここですべての $x\in G$ に対して，$Hxg=Hx$ となるから，$x^{-1}Hxg=x^{-1}Hx$，すなわち $g\in x^{-1}Hx$．したがって，$g\in\bigcap_x x^{-1}Hx=N$．ここで N は明らかに，H に含まれた G の正規部分群である．さらに H に含まれる G の任意の正規部分群は，すべての $x^{-1}Hx$ に含まれるから N に入る．したがって N は H に含まれる G の最大正規部分群である．逆に $g\in N$ ならば，すべての x に対して，$Hxg=Hx$ だから $\pi(g)=1$．$N=1$ となることは，$g\to\pi(g)$ が G の忠実な表現となるための必要かつ十分な条件である．

系 5.3.1. アーベル群の忠実な可移表現は正則表現に限る．

定理 5.3.1. 部分群 H_1 と H_2 の上の G の２個の忠実な表現が，置換群として同型になる必要十分条件は，G の自己同型 α で，$H_1{}^\alpha=H_2$ となるものが存在することである．

証：α を G の自己同型で $H_1{}^\alpha=H_2$ となるものとする．すると，

$$H_1x\leftrightarrows H_1{}^\alpha x^\alpha=H_2x^\alpha$$

は，H_1, H_2 の剰余類の集合の間の1対1対応であって，$g \to \pi_1(g)$, $g \to \pi_2(g)$ がそれぞれ H_1 および H_2 の上への表現ならば，$\pi_1(g) \leftrightarrows \pi_2(g^\alpha)$ となる．

一方，置換同型

$$\pi_1(g) \leftrightarrows \pi_2(g^*)$$

が存在すると仮定する．表現が忠実であるから，1対1の対応 $g \leftrightarrows g^*$ が定義され，これはGの自己同型 β となる．置換同型 $\pi_1(g) \leftrightarrows \pi_2(g^*)$ において，$H_1 \leftrightarrows H_2u$ とする．したがって $H_1g = H_1$ とすれば，

$$H_2ug^\beta = H_2u$$

すなわち

$$u^{-1}H_2ug^\beta = u^{-1}H_2u$$

そして，逆もまた成立する．ゆえに $g \in H_1$ ならば，$g^\beta \in u^{-1}H_2u$ そして，逆もまた成立する．$H_1{}^\beta = u^{-1}H_2u$，すなわち $H_2 = uH_1{}^\beta u^{-1} = H_1{}^\alpha$，ここで α は G の自己同型である．

5.4. 交 代 群 A_n

n 変数の多項式 $\Delta = \prod_{i<j} (x_i - x_j)$; $i, j \leq n$; $n \geqq 2$ を考える．もし $x_1, x_2, \cdots, x_n$ が，それら自身の置換によって置き換えられるならば，Δ は Δ または $-\Delta$ のいずれかになる．

$$\begin{aligned}\Delta = (x_1 - x_2)&(x_1 - x_3)\cdots(x_1 - x_n)\\ &(x_2 - x_3)\cdots(x_2 - x_n)\\ &\cdots\cdots\cdots\cdots\cdots\cdots\\ &\qquad\qquad (x_{n-1} - x_n)\end{aligned}$$

と Δ を分解して書けば，交換 (x_1, x_2) は $x_1 - x_2$ を $x_2 - x_1 = -(x_1 - x_2)$ で置き換え，そして第一列の $(x_1 - x_3)\cdots(x_1 - x_n)$ を第二列で置きかえ，残りはそのままにすることが分かる．したがって置換 (x_1, x_2) は Δ を $-\Delta$ にする．置換が Δ を不変にするとき**偶置換**，Δ を $-\Delta$ にするとき**奇置換**とよぶ．

定理 5.4.1. $x_1, x_2, \cdots, x_n$ 上の偶置換の全体は，対称群 S_n の中で指数2の

正規部分群を形成する．この群は**交代群** (alternating group) A_n とよばれる．

証：二つの偶置換の積は偶置換，二つの奇置換の積は偶置換，偶置換と奇置換の積はいずれの順序にしろ奇置換となることは直接確かめることができる．恒等置換が偶置換であることに注意する．

したがって，S_n の偶置換の全体は部分群 A_n を形成する．(x_1, x_2) は奇置換であるから，剰余類 $A_n(x_1, x_2)$ は奇置換のみを含む．しかし，π を任意の置換とするとき，π と $\pi\cdot(x_1, x_2)$ のいずれか一方は偶置換で，他方は奇置換である．$\pi=[\pi\cdot(x_1, x_2)](x_1, x_2)$ より，A_n と $A_n(x_1, x_2)$ をあわせれば S_n となる．$S_n=A_n+A_n(x_1, x_2)=A_n+(x_1, x_2)A_n$．したがって，$A_n$ は S_n 中指数 2 となるから正規部分群である．

長さ 2 の巡環 (x_i, x_j) は**互換** (transposition) とよばれる．定理 5.1.3 よりすべての互換は S_n 中 (x_1, x_2) と共役になる．π がいずれであっても π と π^{-1} はともに偶置換またはともに奇置換であるから，$\pi^{-1}(x_1, x_2)\pi=(x_i, x_j)$ は奇置換である．すべての互換 (x_i, x_j) が奇置換であることを直接計算することもできる．

$(x_1, x_2, \cdots, x_n)=(x_1, x_2)(x_1, x_3)\cdots(x_1, x_n)$ となるから長さ n のすべての巡環は $n-1$ 個の互換の積である．したがって，有限個の文字の上のすべての置換は互換の積として表わされる（定理 5.1.1）．偶数個の互換の積は偶置換で，奇数個の互換の積は奇置換となる．ゆえに，一つの置換は種々の方法で互換の積として書けるが，含まれる互換の数が偶数か奇数かは決まっている．

定理 5.4.2. $A_n(n\geq 3)$ は $(n-2)$-重可移である．

証：$y_1, \cdots, y_{n-2}, y_{n-1}, y_n$ を $x_1, \cdots, x_{n-2}, x_{n-1}, x_n$ の任意の並び方とする．

$$u=\begin{pmatrix} x_1, \cdots, x_{n-2}, x_{n-1}, x_n \\ y_1, \cdots, y_{n-2}, y_{n-1}, y_n \end{pmatrix},$$

$$v=\begin{pmatrix} x_1, \cdots, x_{n-2}, x_{n-1}, x_n \\ y_1, \cdots, y_{n-2}, y_n, y_{n-1} \end{pmatrix},$$

ならば $v=u(y_{n-1}, y_n)$ で，u, v の一方は偶置換で他方は奇置換である．したがって，A_n は $(n-2)$-重可移であるが，n-重可移ではない．明らかに $(n-1)$

-重可移ではあり得ない.

ω 個の文字の無限集合上の置換群においては，偶数個の互換の積として書ける置換からなる群で交代群 A_ω を定義することができる. A_ω は，有限個の文字のみを置換する置換からなる群 H_ω 中，指数 2 の部分群である. 定理 5.1.3 より H_ω は S_ω の正規部分群であり，A_ω は S_ω の正規部分群で H_ω 中指数 2 である.

定理 5.4.3. 交代群 A_n は，$n=4$ を除く有限または無限の任意の値 n に対して，単純群である.

A_2 は単位群，A_3 は位数 3 の巡回群となるから単純群である. A_4 は別に処理しなければならない. 少なくとも 5 文字あると仮定しよう.

補題 5.4.1. $A_n(n\geq 3)$ は長さ 3 のすべての巡環 (a, b, c) で生成される[1].

証：A_n は 2 個の互換の積であるすべての元によって生成される. もし 2 個の互換が等しければこの積は 1 である. もし一文字を共有すれば，$(a, b)(a, c)=(a, b, c)$. 共通の文字がなければ，$(a, b)(c, d)=(a, b)(a, c)(c, a)(c, d)=(a, b, c)(c, a, d)$. ゆえに補題は証明された.

A_n，$n\geq 5$ に含まれ，単位群より大の正規部分群 G が，長さ 3 のすべての巡環を含むことを証明すれば $G=A_n$ となる. いくつかの場合にわけて処理する. $G\subseteq A_n$ であるから，G のすべての元は有限巡環の有限個の積として書けることに注意しよう.

Case 1. G は長さ 3 の巡環 (a, b, c) を含む.

このとき長さ 3 の他のすべての巡環 (x, y, z) は，(a, b, c) とともに有限個 r の文字の上の交代群 A_r に入る. ここで $r\geq 5$ としてよい. A_r は $(r-2)\geq 3$-重可移だから，(a, b, c) と (x, y, z) は A_r 中共役，したがって A_n 中共役となる. しかし G は正規部分群なので，A_n において (a, b, c) と共役なすべての元を，したがって長さ 3 のすべての巡環を G は含まねばならない. ゆえに

---

[1] $A_n(n\geqslant 4)$ の生成元としては $(1, 2, 3)$，$(1, 2)(3, 4)$，$(1, 2)(4, 5)$，$\cdots$，$(1, 2)(n-1, n)$ を考えると有効な場合が多い.

補題 5.4.1 より $G=A_n$.

Case 2. Gは長さ $s\geq 4$ の巡環をもつ元 g を含む.

$$g=(a_1, a_2, \cdots, a_r)\cdots(c_1, c_2, \cdots, c_{s-3}, c_{s-2}, c_{s-1}, c_s)$$

とする. $t=(c_{s-2}, c_{s-1}, c_s)\in A_n$, かつ

$$t^{-1}gt=(a_1, a_2, \cdots, a_r)\cdots(c_1, c_2, \cdots, c_{s-3}, c_{s-1}, c_s, c_{s-2})$$

しかし, $gt^{-1}g^{-1}t=(c_{s-3}, c_s, c_{s-2})$ は, Gが正規なのでGに属する. したがって, Case 1 に帰着された. 巡環の長さが3より大でない場合を考えよう.

Case 3. Gのある元 g が長さ3の巡環を2個以上含む.

$$g=(a_1, a_2, a_3)(b_1, b_2, b_3)\cdots(c_1, \cdots, c_r)$$

$t=(a_3, b_1, b_2)\in A_n$ とすれば,

$$h=t^{-1}gt=(a_1, a_2, b_1)(b_2, a_3, b_3)\cdots(c_1, \cdots, c_r)\in G,$$

かつ

$$gh^{-1}=(a_2, b_2, a_3, b_1, b_3)\in G.$$

したがって, Case 2 に帰着される.

Case 4. Gのある元 g が長さ3の巡環を少なくとも1個含み, 他の巡環は長さ 2.

$$g=(x_1, x_2)(y_1, y_2)\cdots(z_1, z_2)(a, b, c)\cdots(d, e, f).$$

$$g^2=(a, c, b)\cdots(d, f, e)\in G.$$

したがって, Case 1 または Case 3 に帰着された.

Case 5. Gのある元 g が長さ2の巡環のみを含み, しかも4個以上含む.

$$g=(x, y)(z, u)\cdots(a, b)(c, d)\in G.$$

$t=(y, a)(b, c)\in A_n$ をえらぶ.

$$h=t^{-1}gt=(x, a)(z, u)\cdots(y, c)(b, d)\in G$$

$$gh=(x, c, b)(y, a, d)\in G$$

したがって, Case 3 に帰着される.

Case 6. $g\in G$ が長さ2の巡環のみを2個含む.

$$g=(a, b)(c, d)\in G$$

$n \geq 5$ より，動かす文字の集合にある文字 e が存在して，$e \neq a, b, c, d$.

$$t=(a, b, e) \in A_n$$
$$h=t^{-1}gt=(b, e)(c, d) \in G$$
$$gh=(a, e, b) \in G$$

したがって，Case 1 に帰着された．

1, 2, 3, 4 上の交代群 A_4 は，位数 4 の正規部分群 {(1), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)} を含む．

5.5. 非可移群．部分直積

置換群 G が非可移であるとし，集合 $S_i(x_{i1}, \cdots)$, $i \in I$, を可移域とする．S_i 以外のすべての文字を無視すれば，集合 S_i 上の置換はそれ自身群 G_i を構成する．各 $i \in I$ に対して，G の元 g は，g が引きおこす S_i の文字の置換 $g_i \in G_i$ を決定する．さらに g を G_i のカルテジアン積の元と見なせば，

$$g=\prod_i g_i \tag{5.5.1}$$

と書ける．なぜならば，G における群の演算は，カルテジアン積 $\prod_i G_i$ における演算と一致するからである．したがって，非可移群は可移群のカルテジアン積の部分群と見なせる．ここで G は，群 G_i の**部分直積** (subdirect product) とよばれる．もっと正確にいえば，(1) G が G_i のカルテジアン積の部分群であり，そして (2) 各 $g_j \in G_j$ に対して，$g \in G$ が少なくとも一元存在して，g_j を第 j 番目の成分として持つときに群 G は G_j の部分直積とよばれる．この第 2 番目の条件は群 G_i のすべての元が実際に G の表示に表われることを要求している．

部分直積 $G \subseteq \prod_i G_i$ において，すべての成分 g_i が独立に現われるならば，G はカルテジアン積の全体と一致する．このことは一般には正しくないが，次の定理は，部分直積の成分の間に生ずるある種の関係を述べている．G_i, G_j を二つの成分，すなわち成分 $G_i, i \in I_1$, $G_j, j \in I_2$, $I_1 \cap I_2 = 0$ の共通部分のない集合によって決定された群とする．G_i, G_j 以外のすべての成分を無視すれ

ば，Gの元はG_iとG_jの部分直積の群G^*を決める．我々は，G_iとG_jから誘導された部分直積G^*を正確に述べることによって，Gにおける成分G_iとG_jの関係を記述できる．

定理 5.5.1. G^*を群G_iとG_jの部分直積とし，H_{ij}をG_jの単位元との組であるG_iの元の集合とし，H_{ji}も同様に定義する．すると，H_{ij}, H_{ji}は各々G_i, G_jの正規部分群で，$G_j/H_{ij} \cong K \cong G_j/H_{ji}$となる同型が存在し，$(g_1, g_2)$, $g_1 \in G_i, g_2 \in G_j$がG^*の元である必要十分条件は準同型$G_i \to K$，$G_j \to K$において，g_1とg_2が同じ像kを持つことである．

証：G^*においてG_jの単位元との組であるG_iの元$(h, 1)$の集合H_{ij}は，明らかにG_iの正規部分群であり，同様にして，G^*において$(1, h)$という形をした元の集合H_{ji}は，G_jの正規部分群である．さらに，$g_1 \in G_i$に対して，固定元g_1とともに生ずる元$g_2 \in G_j$の集合は，H_{ji}の剰余類の一つである．同様に，固定元g_2とともに生ずるg_1の集合は，H_{ij}の剰余類の一つである．さらに，(g_1, g_2)がG^*に属するならば，$(H_{ij}g_1, H_{ji}g_2)$という形のすべての元はG^*に入る．そしてG^*の他のどんな組(g_1', g_2')も成分としてこれらの元のどの一つも含まない．したがって，各(g_1, g_2)に対して，G_iにおけるH_{ij}の剰余類と，G_jにおけるH_{ji}の剰余類の間に，1対1の対応$H_{ij}g_1 \rightleftarrows H_{ji}g_2$が決められた．

(g_1, g_2), (g_3, g_4)がG^*に入れば，(g_1g_3, g_2g_4)もG^*に入る．そして，この対応は積を保ち，それゆえ，剰余群G_i/H_{ij}とG_j/H_{ji}の間の同型でなければならない．ここで$G_i/H_{ij} = K = G_j/H_{ji}$と書く．そして，$(g_1, g_2)$が$G^*$に入れば，$g_1, g_2$は対応する剰余類に入ることが分かる．したがって，$g_1$と$g_2$は$G_i, G_j$の準同型像$K$において同じ像を持つ．

逆に，2つの群G_iとG_jが各々正規部分群H_{ij}, H_{ji}を持ち，$G_i/H_{ij} = K = G_j/H_{ji}$ならば，準同型$G_i \to K$，$G_j \to K$において，$g_1 \to k$, $g_2 \to k$となる$g_1 \in G_i$, $g_2 \in G_j$のすべての組(g_1, g_2)は，上のように部分直積G^*を構成する．

5.6. 原　始　群

$G \neq 1$ をある文字の上の置換群とし，その文字の集合が交わらない集合 $S_1, \cdots, S_m$ に分割され，Gの引き起こすすべての置換は，S_i のすべての文字を S_i の上に移すか，あるいは，他の集合 S_j の文字の上に移すと仮定する．このとき，集合が唯一つの場合，および各集合がただ一つの元からなるという特殊な場合を除き，Gは**非原始群**（imprimitive group）とよばれる．そして，$S_1, \cdots, S_m$ を**非原始類**とよぶ．したがって，非可移群は非原始群である．もしGが非原始群でないならば，Gを**原始群**（primitive group）とよぶ．ゆえに，原始群は可移群であって，その文字の集合は，互いに移りあう真の部分集合の和には分割できない．

定理 5.6.1. Gを可移かつ非原始群とする．S_1 を非原始類の一つとし，y_1 を S_1 の一つの文字，Hを y_1 を固定する元からなる部分群とする．このとき，S_1 を S_1 に移すGの元は，GとHの間に真に含まれる部分群Kを構成する．非原始類の数は指数（$G:K$）に等しく，非原始類の各集合はすべて同じ数（$K:H$）の文字を含む．逆に，Gを可移群として，Hを文字 y_1 を固定する部分群とする．もし $G \supset K \supset H$ となる部分群Kが存在するならば，Gは非原始群で，非原始類の一つは（$K:H$）個の文字からなり，Kの元はそれらの文字の中に y_1 を移す．Kの左剰余類に対応する（$G:K$）個からなる非原始類がある．したがって，置換群Gが原始群であるための必要十分条件は，一文字を固定する部分群Hが極大部分群となることである．

証：Gが可移かつ非原始群と仮定する．$S_1, \cdots, S_m$ をGに対する非原始類とし，Hを S_1 の文字 y_1 を固定する部分群とする．すると

(5.6.1)
$$G = H + Hx_2 + \cdots + Hx_n$$

ならば，定理 5.3.1 より，Gによって置換される文字 $y_1, y_2, \cdots, y_n$ を $\pi(g): Hx_i \to Hx_i g,\ g \in G$ によって置換される（5.6.1）の左剰余類の集合 Hx_i と見なすことができる．$y_1, y_2, \cdots, y_t$ が S_1 の文字とすれば，これらの文字の間

の置換を引き起こすGの元は部分群Kを構成する．y_1を固定するGの元は S_1 を S_1 に移さねばならないから，$H\subset K$．y_1 を y_2 に移す元はKに入るがHには入いらないから，真の包含関係が成立する．Kは S_1 上可移である．したがって，

$$K=H+Hx_2+\cdots+Hx_t, \tag{5.6.2}$$

そして，S_1 の文字の数 t は $(K:H)$ であることが分かる．S_1 はGによってうごかされる文字をすべては含み得ないから，KはGの真の部分群である．S_i を非原始類の任意の一つとすれば，y_1 を S_i の文字に移すGの元が存在するから，S_1 のすべての元は S_i の上に移され，したがって，S_i は S_1 と同数の文字を含む．さらに，置換 $Hx_i\to Hx_ig$ において，$Kx_i\to Kx_ig$，したがって，非原始類は (5.6.1) におけるKの左剰余類の集合と見なされ，ゆえに，それらは $(G:K)$ 個存在する．

逆に，Gを文字 y_1 を固定する部分群Hによる剰余類の集合上の置換 $Hx_i\to Hx_ig$ によって与えられる可移群と仮定する．さらに，$G\supset K\supset H$ となる部分群Kが存在すると仮定する．するとKの剰余類は，Hの剰余類の集合からなり，これらはGに対する非原始類をなす．したがって，Gが原始群である必要十分条件は，部分群Hが極大となることである．

原始群の定義およびこの定理から生ずるいくつかの基本的な注意を述べる．2重可移群は原始群である．なぜならば，S_1 を2重可移群Gによって置換される文字の一部からなる任意の集合とすれば，S_1 の一元を S_1 の中に移し，S_1 の他の元を S_1 の外に移す置換が存在するからである．第2番目に，n次の群（置換群の次数はそれがうごかす文字の数のことである）は t が n の約数のときだけ t 個の文字の非原始類を持つことができる．なぜならば定理5.6.1において，$n=(G:H)$，$t=(K:H)$ であるからである．ゆえに素数次の群は確かに原始群である．p-群においてはすべての部分群は指数 p の極大正規部分群に含まれる（系4.2.2）．したがって，p-群である置換群は，p 個の文字の上の置換群でなければ非原始群であり，そうである場合には，それは p 次の巡回群となる．

定理 5.6.2. Gをn文字上の原始置換群とし，Hをm文字上のGの可移部分群で，残りの $n-m$ 文字を固定するものとする．すると，（1）Hが原始群ならば，Gは $n-m+1$ 重可移である．（2）いずれにせよ，Gは2重可移である．

証：Hはm文字上可移である．Hの各共役部分群はあるm個の文字上可移であり，Gは可移群であるから，すべての文字はこれらの集合の少なくとも一つにあらわれる．もしこれらの集合が一致するか，または交わらなければ，これらはGに対する非原始類である．したがってHの共役部分群で，Hと作用する文字（すべてではない）を共有するものがある．H'をこのような部分群の一つで，Hと共通な文字を最も多く共有するものとする．

$$(5.6.3)\qquad H:(a_1,\cdots,a_r,c_1,\cdots,c_s);\quad H':(b_1,\cdots,b_r,c_1,\cdots,c_s),\ r+s=m$$

上の記号で，我々は，c_i はH と H' がともに動かす文字，r 個の a_i はHが，r 個の b_i は H' がそれぞれ動かすものとする．Hが原始群ならば，$r=1$，Hが非原始群で $r>1$ ならば，$a_1,\cdots,a_r$ はHに対する非原始類であることを証明する．H' の元 h' を次のように書く．

$$(5.6.4)\qquad h'=\begin{pmatrix} b_1, \cdots, b_u, b_{u+1}, \cdots, b_r, c_1, \cdots, c_{r-u}, c_{r-u+1}, \cdots, c_s \\ b\ , \cdots, b\ , c\ \ \ \ , \cdots, c\ , b\ , \cdots, b\ \ \ \ , c\ \ \ \ \ \ \ , \cdots, c \end{pmatrix}$$

ここで，u 個の文字 b_i は b の上に，$b_i(u+1\leqslant j\leqslant r)$ は c の上に，$c_k(1\leqslant k\leqslant r-u)$ は b の上に，そして $c_l(r-u+1\leqslant l\leqslant s)$ は c の上にうつることを示している．(5.6.4) の h' の第2行には，r 個の b が存在しなければならないから，c の上に移る b の数 $r-u$ は，b の上に移る c の数に等しいことに注意する．したがって $h'^{-1}Hh'$ は，r 個の a，$(r-u)$ 個の b，$(s-r+u)$ 個の c を置換し，ゆえにHと $s+u$ 個の文字を共有する．ゆえに，もし $r>1$ で H' が原始群ならば，b のすべてではなくいくつかをそれら自身の中に移す元として h' を選べるから，$1\leq u<r$；したがって，$h'^{-1}Hh'$ はHと $s+u$ 個の文字を共有し，それは s より多く $r+s=m$ よりは少ない．いずれにせよ，Hが原始群のときは，$r=1$ でなければならなく，そしてまた H が原始群であるか否かにかかわらず，もし $r=1$ ならば，$H\cup H'$ は $m+1$ 文字上2重可移となるから原始

群である．この操作をGに到るまで続けることができ，次々に，$m+1$ 文字上の2重可移群，$m+2$ 文字上の3重可移群を得て，結局Gは $n-m+1$ 重可移群となる．

Hが非原始群の場合は，この方法は適用できない．しかし，$b_1, \cdots, b_r$ が H' に対する非原始類でなく，$a_1, \cdots, a_r$ がHに対する非原始類でないならば，H と H' が共有する文字の数sを増すことができることに注意する．さらに，$H \cup H'$ は $s+2r=m+r$ 文字上の可移群である．したがって，mがたかだか $n/2$ ならば，$m+r$ はnより小となる．我々は，$n/2$ より大きくnより小さいm個の文字の上の可移部分群Hが得られるまで文字を次々に増やして可移部分群を構成することができる．この場合，Hの任意の共役部分群 H' は，Hと共通の文字のいくつかを動かす．ここで，Hがnより小さい最大の文字の上の可移群と仮定する．$s+2r=n$ かつ $r=1$ ならば，Hは $n-1$ 文字上可移であるからGは2重可移群となる．もしこのようなことが起こらなければ，$s+2r=n$, $r \neq 1$ でHに到達する．このとき，a, b, c はすべてGの文字である．しかしGは原始群であるから，ある元gが存在してb_1をb_iに移すが，すべてのbをそれらの中には移さない．したがって少なくとも一つのaまたはcをbに移す．ここで，Hと $g^{-1}Hg$ はどちらもb_iを固定し，それらの和はHよりも多くの文字の上で可移である．したがって最終的には $n-1$ 文字上で可移な部分群に到達しなければならないから，Gは2重可移群である．

定理の二者択一が実際に起こる．第一章の例4はこのことを説明している．そこでは，群は7文字上可移，したがって原始群である．それは4文字 C, E, F, G 上の可移部分群を持ち，2重可移ではあるが3重可移ではない．

5.7. 多重可移群

n文字上の対称群は勿論n重可移である．そして交代群 A_n (5.4 で注意したように) は $(n-2)$ 重可移である．我々は多重可移群の議論において A_n, S_n を除外する．3重可移群は無限に存在する．しかし交代群と対称群を除けば4

重可移で知られている群はわずかに4個しかない．これらはそれぞれ，11, 12, 23, 24, 文字上のMathieu群で，12と24文字上の群は5重可移群で一文字を固定する部分群として，それぞれ11と23文字上の群を含んでいる．これらの不思議な群はかなり研究されてきたが，例外的なものか，あるいは4重可移群の無限系列の一員なのかは知られていない．

Miller [1] による定理 5.7.1 は次数 n の群の可移性の限界を与えている．この定理と Bertrand の仮定をあわせると，$n>12$ に対して次数 n の群は $t\geq 3\sqrt{n}-2$ に対して t 重可移群ではあり得ないことが証明される．Bertrand の仮定（Chebyshev によって1850年に証明された．）とは次のようなものである．$x\geqq 7$ となる任意の実数に対して，$x/2<p\leq x-2$ となる素数 p が存在する．Miller の定理は n の非常に特定な値に対してかなりよい限界を与えている．さらによい制限が知られているがその証明はここで述べるには複雑すぎる*)．

定理 5.7.1. Gをn文字上のt重可移群とする．Hをt個の文字を固定する部分群とする．そしてPをHの Sylow p-部分群とし，Pは $w\geq t$ 個の文字を固定するとすれば，PのGにおける正規化群は P によって固定される w 個の文字の上に t 重可移である．

証：$a_1, \cdots, a_t$, と $b_1, \cdots, b_t$ を t 個の文字からなる2つの順序ある集合とする．両者ともPによって固定されるw個の文字から選んだものとする．Gはt重可移だからGの元xが存在して a_i を b_i に移す．$i=1, \cdots, t$. したがって，$x^{-1}Px$ は $b_1, \cdots, b_t$ を固定する．そしてPと $x^{-1}Px$ は $b_1, \cdots, b_t$ を固定する群の Sylow 部分群である．第2 Sylow 定理によって，これらの群は $b_1, \cdots, b_t$ を固定する群の中で共役でなければならない．ゆえにある元yが存在し，yは $b_1, \cdots, b_t$ を固定し，$y^{-1}(x^{-1}Px)y=P$ となる．しかしここで $z=xy$ とおけば，z は $a_1, \cdots, a_t$ を $b_1, \cdots, b_t$ に移し，$z^{-1}Pz=P$. したがってPによって固定されるw個の文字の中から選んだ2つの任意の t 個の文字の集合を互いに

*) E. Parker は t に対して $\sqrt[3]{n}$ 位の評価を得た．最もよい評価は Wielandt [1] による $t<3\log n$ である．

移す元がPのGにおける正規化群の中に存在することが分かったから，PのGにおける正規化群はPによって固定されるw個の文字の上にt重可移である．

定理 5.7.2. 整数を $n=kp+r$ とする．pは素数で $p>k$，$r>k$ とする．$k=1$，$r=2$ を除けば，次数nの群は S_n や A_n でなければ $(r+1)$ 重可移ではあり得ない．

証：次数nの群Gが $(r+1)$ 重可移とする．はじめのr個の文字 $1, 2, \cdots, r$ を固定する部分群Hは残りの kp 個の文字の上に可移である．したがってHの位数は素数pで割り切れる．そして，Sylow p-部分群Pを含む．一文字を固定するHの部分群はH中指数 kp であるからその位数はHの位数を割り切るpの最高巾では割れない．ゆえにPはHが可移である kp 個の文字のすべてをうごかさなければならない．さらに仮定によって $kp<p^2$ だからPは p^2 個の文字の上の可移成分を含むことはできない．Pの可移域の文字の数はPの位数の約数であるからPはHの kp 個の文字の上にp個の文字からなるちょうどk個の可移域をもたねばならない．（我々は一文字からなる可移域を除いていた．）これらの各可移域の上でPは位数pの巡回群でなければならない．したがってPはp個の文字の上の位数pのk個の巡回群の部分直積である．ゆえにPのすべての元は位数pでPはアーベル群である．しかし我々はPが部分直積であるということはあまり取り扱わないであろう．

NをPのGにおける正規化群とする．定理 5.7.1 より，NはGの最初のr個の文字の上の対称群 S_r である．はじめに $r\geq 5$ の場合を考える．そして N_1 をNの部分群ではじめのr個の文字の上の交代群とする．定理 5.4.3 より A_r は位数 $r!/2$ の単純群である．そしてアーベル群ではない．$T_1, \cdots, T_k$ をPのp個の文字からなるk個の可移域とする．すると，はじめのr個の文字の上の置換と，可移域 T_i の上の N_1 による置換を結合すれば N_1 の準同型像が与えられる．この像ははじめのr個の文字の上の A_r とk個の T_i をうごかす群との部分直積である．しかし，k個の文字の上の群の位数はたかだか $k!$ であるから，$k!<r!/2$ より単純群 A_r と同型な剰余群を持ち得ない．したがって A_r

の剰余群と同型なこの群の剰余群は単位群だけである．それゆえ，A_r と可移域 T_i を含むこの群は 5.5 の結果より A_r と他の群の直積となる．ここで A_r と他の群の単位元は N_1 における逆像として，はじめの r 個の文字の上の A_r である群 N_2 を持ち，それは各可移域 T_i の文字をそれらの間でうごかす．N_2 を調べるために $a=(x_1, \cdots, x_p)$ で生成された p 個の文字の上の巡回群の正規化群の性質を考えねばならない．$a^p=1$ より $b^{-1}ab=a^i$ から $c^{-1}ac=a^j$ ならば bcも cb も a を a^{ij} に移す．したがって，変換によって巡回群の上に引き起こされる自己同型はアーベル群を構成する．（次の章で，位数 p の巡回群の自己同型はそれ自身位数 $p-1$ の巡回群であることが分かる．）

a と可換な $x_1, \cdots, x_p$ 上の元 u は a の適当な巾 a^i をかけると，$v=ua^i$ となり，これは a と可換で x_1 を固定する．しかし $a^{-1}va=v$ かつ v は x_1 を固定するから v は $x_2, \cdots, x_p$ を固定し，$v=1$ となることが容易に分かる[1]．したがって $u=a^{-i}$ である．N_2 は P の p 個の文字からなる k 個の 可移域 T_i の一つの上で p 個の文字の巡環の巾からなる位数 p の正規部分群をもつ．そして，位数 p の群の上に異なる自己同型を引き起こす元からなる剰余群を持つ．この剰余群はアーベル群である．したがって，この群の任意の剰余群はアーベル群か可換な剰余群を持つ．それゆえ A_r の剰余群と 同型な 剰余群は 単位群だけである．したがってしばらくの間 $T_2, \cdots, T_k$ を無視する．5.5の結果をはじめの r 文字と T_1 に適用すれば N_2 ははじめの r 文字の上で A_r で T_1 の文字の上で単位群となる部分群を持つ．この N_2 の部分群 N_3 ははじめの r 文字の上で A_r で T_1 と T_2 の上で単位群となるような部分群 N_4 を持つ．

この操作を繰り返すと，我々は，はじめの r 文字の上で A_r であって，残りの文字の上で単位群となる部分群を得る．しかし A_r は 3 文字上の巡環 (a, b, c) を含む．そして G は少なくとも n 文字上 5 重可移であるから，この巡環は n 文字の上の任意の 3 文字の巡環に変換できる．補題 5.4.1 よりこれらの 3 次巡環は A_n を生成する．そして G は A_n を含むから G は A_n または S_n である．

---

1) $v=(x_1)\cdots\cdots$ とあらわせるから $v=a^{-j}va^j=(x_j)\cdots\cdots$ となって，v は $x_1, \cdots, x_p$ を固定することになる．

上に述べた議論は $r \geq 5$ のとき通用する．そして，$r=3$, $k=1$ または2および $r=4$, $k=1$, 2, または3の場合を考えねばならない．まずはじめに，P が a から生成された巡回群で $k=1$ または2の場合を考えよう．上に注意したように $u=(12)(3)\cdots$ と $v=(1)(23)\cdots$ が P の正規化群 N の元ならば(これは P によって固定されたはじめの3文字または4文字の上の対称群であるが) P が巡回群だから uv と vu は a を a の同じ巾に変換する[1]．したがって $u^{-1}v^{-1}uv=(1,2,3)\cdots$ は a と可換である．この元 $w=u^{-1}v^{-1}uv$ は2個の可移域 T_1, T_2 を交換するか，両者をそれ自身の中にもっていく．いずれにせよ $w^2=(1,3,2)\cdots$ は両方の可移域を固定する．この元は位数が3で割れるからある適当な巾は位数が 3^s となり，はじめの3文字の上の3次巡環となり，可移域を可移域に移し，a と可換である．しかし a の巡環に対して可換な元はその巡環の巾で，それらが単位元でなければ位数 p である．したがって，$p \neq 3$ ならば a と可換な位数 3^s の元ははじめの3文字上の3次巡環 $(1,2,3)$ または $(1,3,2)$ と残りの文字上の単位元である．ゆえに G は3次巡環を含み，3重可移であるから A_n または S_n でなければならない．$p=3$ のときを除外していた．これは，$n=6,7,9,10$ に対して $k=1$ または2そして $r=3$ または4である．実際 $p=3$, $k=1$ で P 自身3次巡環であるから結論は得られる．これは $n=6,7$ を解決している．$n=9,10$ は特殊な場合としてあつかう．$k=1$ となるすべての場合がここで含まれている．なぜならば P は巡回群だからである．$k=2$, かつ P が巡回群でないとすれば，P は2個の p 次巡環の直積である．そして，定理 5.6.2 を G が原始群であり，H は位数 p の巡環を持つことと ともに適用する．ここで G は $(p+4)$ または $(p+5)$ 重可移である．そして $r=p+3$ または $p+4$, $k=1$ を用いて $G=A_n$ または S_n となる．

$k=3$, $r=4$ の場合を考える．はじめに P が巡回群ならば，以前のように $(1,2,3)(4)\cdots(1)(2,3,4)\cdots$ という元が存在し，実際はじめの4文字の上のすべての8個の可能な3次巡環は P の生成元 a と可換になる．しかしこれらは a の3個の可移域を (T_1, T_2, T_3) または (T_1, T_3, T_2) のどちらかの方法で巡回

[1] 巡回群の自己同型群はアーベル群となるからである．

的にうごかし，8個のうち少なくとも2個は T_i を同じ方法でうごかさねばならない．これらのことを総合して，我々は T_1, T_2, T_3 をこの中でうごかす元 $(1,2,3)(4)\cdots$ または $(1,2)(3,4)\cdots$ を得る．p は少なくとも5であり，a と可換で a の巡環をこれらの形の一つの中に移す元は a の $3p$ 個の文字を固定する同じ形の元を導く．したがって G は3次巡環 $(1,2,3)$ または元 $(1,2)(3,4)$ を持つ．そして4重可移性によって $(1,2)(3,5)$ と $(3,4,5)$ を含む．ゆえに G は A_n を含み，A_n または S_n となる．一方 P が p 文字の一つの巡環を含めば，定理 5.6.2 を適用して，G は $(2p+4)$ 重または $(2p+5)$ 重可移群となるから再び A_n または S_n である．

最後の場合として P が巡回群でなく，また p 次巡環を含まない可能性を考えなければならない．このとき P の位数は p^2 である．2元 $a=(x_1, x_2, \cdots, x_p)(y_1, \cdots, y_p)$, $b=(y_1, \cdots, y_p)(z_1, \cdots, z_p)$ を P の基底とすることができる．したがって ab^{-1} とその巾のみが文字 y からなる成分 T_2 を固定する P の元である．$(1,2,3,4)\cdots$ という形の P を正規化する元は3個の成分を固定するか，その中の2個をうごかし残りの1個を固定する元である．したがって，その平方，$u=(1,3)(2,4)\cdots$，は3個の成分のすべてを固定する．それゆえ，u は a, b, ab^{-1}，をそれ自身のある巾に移す．特に a と b を a, b, の同じ巾たとえば i 巾に移す．すなわち P のすべての元をその i 巾にうつす．そのような自己同型は P の他のすべての自己同型と可換でなければならない．そして，とくに $w=(1)(2,3)(4)\cdots$，によって引き起こされる自己同型と可換である．それゆえ，$v=w^{-1}uw=(1,2)(3,4)\cdots$ は P のすべての元をその i 巾に移すから，P の成分を固定する．しかし，$uv^{-1}=(1,4)(2,3)\cdots$ はその成分を固定する P のすべての元と可換である．このことから $(1,4)(2,3)$ という元が G に存在する．そして G は4文字より多くの文字の上に4重可移であるから，G は再び A_n または S_n となる．

5.8. Jordan の定理[1]

1872年に Jordan [2] は有限4重可移群で4文字を固定する元が単位元に限るものは次の群のいずれかであることを示した．すなわち，4次または5次の対称群，6次交代群，または11文字上の Mathieu 群．

Jordan の4重可移群に関する定理はここでは2つの方法で一般化される．文字の数は有限とは仮定しない．すなわち，4文字を固定する部分群が単位元だけからなることを仮定するかわりに，それが奇数位の有限群であるということだけを仮定する．結論は本質的には Jordan の結果と同じであるが，この仮定を満たす群に7次交代群も含まれる．

定理 5.8.1. 有限個または無限個の文字の上の4重可移群をGとする．4文字を固定する部分群Hが奇数位数[2] とすればGは S_4, S_5, A_6, A_7 または11文字上の Mathieu 群のいずれかである[3]．

Case 1. Gが7文字以下の文字上の群とする．4または5文字上の4重可移群は対称群でなければならない．6文字上ではその位数は少なくとも $6\cdot5\cdot4\cdot3$ でなければならない．それゆえ A_6 または S_6 である．7文字上ではその指数はたかだか S_7 中6である．S_7 は指数3または6の部分群を持たない[4] から，残る可能性は A_7 と S_7 である．S_6 と S_7 において少なくとも4文字を固定する位数2の元が存在する．それゆえ，これらの群は我々の仮定を満たさない．

Gが7文字より多くの文字に作用しているのを取り扱うために次の補題からはじめよう．

補題 5.8.1. 次の関係式を満たす元aとbで生成される群は位数 $2s$ の二面

---

1) Jordan の定理は Nagao によって拡張された．

2) Gの位数2の元がたかだか3文字を固定するといい換えてもよい．

3) Nagao による拡張は次のとおりである．G を有限個の文字上の4重可移群とする．Gの位数2の元がたかだか5文字を固定するならば，Gは定理 5.8.1. のいずれかの群かまたは S_6, S_7, A_8, A_9, 12文字上の Mathieu 群，である．

4) 第16章，誘導表現を用いて，容易に確かめることができる．

体群である.

$$a^2=1,\ b^2=1,\ (ab)^s=1$$

$s=2t-1$ ならば $y=ab$ の巾は a を b に移す. $s=2r$ ならば a と b は y^r と可換となる.

証：$y=ab$ より

$$a^2=1,\ y^s=1,\ b=ay=y^{-1}a.$$

$s=2t-1$ ならば

$$y^{-t}ay^t=ay^{2t}=b$$

$s=2r$ ならば

$$ay^r=y^{-r}a=y^ra.$$

これからさき，Gは7文字より多くの文字上の4重可移群とし，Hを4文字を固定する奇数位数mの部分群とする.

補題 5.8.2. Gは位数2の元を含み，位数2の元はすべて共役である.（1）位数2のすべての元は2文字を固定するか，（2）位数2のすべての元は3文字を固定するか，のどちらかである.

証：Gは4重可移だから

$$g=(12)(34)\cdots$$

となる元を含む. g^2 は 1, 2, 3, 4 を固定する. それゆえ g^2 はHに含まれるから有限奇数位数 m_1 である. したがって,

$$x=g^{m_1}=(12)(34)\cdots$$

$x^2=1$ である. Hは奇数位数だから，任意の位数2の元はたかだか3文字を固定するにすぎない. それゆえ，少なくとも4文字をうごかす.

$$u=(ab)(cd)\cdots$$

とすれば，u の共役元

$$v=w^{-1}uw=(12)(34)\cdots$$

が存在する. $v=x$ または vx は4文字を固定し奇数位数である. したがって補題 5.8.1 より v と x は共役である. ゆえに，位数2の元はすべて共役とな

る．一方Gには $z=(1)(2)(34)\cdots$ となる元が存在する．そしてzまたはzの奇数巾は少なくとも２文字を固定する位数２の元である．したがってすべての位数２の元は２文字または３文字を固定する．なぜならば，これらの元は少なくとも２文字を固定するが４文字を固定しないからである．

Case 2. Gが７文字より多くの文字の上に作用しているとき．

$$a_1=(1)(2)(34)\cdots,$$

を位数２の元，そして

$$b=(12)(34)\cdots,$$

を他の位数２の元とする．$f=a_1b=(12)(3)(4)\cdots$ は偶数位数の元で，f^2 は奇数位数m_1となる．したがって $f^{m_1}=a_3$ は位数 2，そして補題5.8.1よりa_1と可換になる．ゆえにGにおいて $a_2=a_1a_3$ と可換な元が存在する．

$$a_1=(1)(2)(34)\cdots,$$
(5.8.1)
$$a_2=(12)(34)\cdots,$$
$$a_3=(12)(3)(4)\cdots.$$

位数２の元としてa_2は２文字５と６，または，３文字５，６，７を固定するかのどちらかである．a_1はa_2と可換だから，これらの文字をその中に移す．しかしa_1は１と２を固定し，そしてたかだかあと１文字を固定する．したがって，

$$a_1=(1)(2)(34)(56)\cdots,$$
$$a_2=(12)(34)(5)(6)\cdots,$$
$$a_3=(12)(3)(4)(56)\cdots,$$

(5.8.2) または

$$a_1=(1)(2)(34)(56)(7)\cdots,$$
$$a_2=(12)(34)(5)(6)(7)\cdots,$$
$$a_3=(12)(3)(4)(56)(7)\cdots.$$

第１の場合は位数２の元がすべて２文字を固定するとき生ずる．第２の場合は３文字を固定するとき生ずる．(5.8.2) の元 a_1, a_2, a_3, と単位元は四元群Vを

なす.

$$
(5.8.3)\qquad
\begin{aligned}
a_1&=(1)(2)(34)(56)(7)(hi)(jk)\cdots,\\
a_2&=(12)(34)(5)(6)(7)(hj)(ik)\cdots,\\
a_3&=(12)(3)(4)(56)(7)(hk)(ij)\cdots,
\end{aligned}
$$

ここで7はないかもしれない.

h, i, j, k を相互にうごかす部分群Kの位数は $24m$ でこれらの文字を固定する位数mの群 $H=H(h, i, j, k)$ はKの正規部分群である. h, i, j, k が次の方法でうごかされる部分群 $U, K\supset U\supset H$ が存在する.

$$
(5.8.4)\qquad
\begin{aligned}
&(h)\\
&(hi)(jk)\\
&(hj)(ik)\\
&(hjik)\\
&(hkij)\\
&(hi)(j)(k)\\
&(h)(i)(jk)
\end{aligned}
$$

Uの位数は $8m$ でUの 2-Sylow 部分群の位数は8である. h, i, j, k を相互に一つの方法でうごかす元はUにおけるHの剰余類である. HはUの正規部分群だからUの位数8の部分群は, 各剰余類からの1元を含む. そして, U/H と同型である. それゆえこれらの文字の上に忠実に表現される. VはUの位数8の Sylow 部分群に含まれる. このことより

$$
(5.8.5)\qquad
\begin{aligned}
a_1&=(1)(2)(34)(56)(7)(hi)(jk)\cdots,\\
a_2&=(12)(34)(5)(6)(7)(hj)(ik)\cdots,\\
a_3&=(12)(3)(4)(56)(7)(hk)(ij)\cdots,\\
u&=(1)(2)(3546)(7)(hjik)\cdots,\\
a_1u&=(1)(2)(3645)(7)(hkij)\cdots,\\
a_2u&=(12)(36)(45)(7)(hi)(j)(k)\cdots,\\
a_3u&=(12)(35)(46)(7)(h)(i)(jk)\cdots,
\end{aligned}
$$

または, 5と6を交換した置換となる. 最後の4元が文字 $1, \cdots, 7$ をうごかす

方法は関係式

$$u^2=a_1,\ \ u^{-1}a_2u=a_3,\ \ (a_2u)^2=1.$$

によって決定される．ここで，uはVを正規化し，それゆえもし7が生ずるならばVによって固定される唯一つの文字7を固定する．またuはa_3で固定される文字をa_2で固定される文字に移さねばならない．したがって，

$$u=\begin{pmatrix}3, 4, \cdots\\ 5, 6, \cdots\end{pmatrix} \quad \text{または} \quad u=\begin{pmatrix}3, 4, \cdots\\ 6, 5, \cdots\end{pmatrix}$$

しかし，また$u^2=a_1$だから

$$u=(3546)\cdots \quad \text{または} \quad u=(3645)\cdots.$$

最後にuは1と2を固定するかこれらを交換せねばならない．しかし，もしuが1と2を交換すればa_2uは位数2，そして文字$1, 2, j, k$を固定する．したがって

$$u=(1)(2)(3546)\cdots \quad \text{または} \quad u=(1)(2)(3645),$$

となる．

h, i, j, kのようなVの可移成分は(5.8.5)におけるような群Sを作る．これらの群の元

$$(12)(36)(45)\cdots \quad \text{と} \quad (12)(35)(46)\cdots$$

はその成分の2文字を固定する．位数2の元は4文字を固定することはできないから，各成分ははじめの6文字を(12)(36)(45)のようにうごかす異なる元をつくる．しかし，はじめの6文字の上にこのように作用する元はたかだかm個しか存在しない．したがってもしt個のこのような成分が存在するならば$t\leq m$は有限そしてGは$n=4t+6$または$4t+7$文字の上に作用している群である．もしGが10または11文字の上に作用していれば$t=1$である．

A_{10}とS_{10}を除けば10文字上の4重可移群は存在しない．なぜならば定理5.7.2によって，7次の巡環の正規化群は残りの3文字上の対称群である．そしてS_3と7次の巡環の文字の上の正規化群の部分直積であるこの正規化群は3次巡環と単位元の組である．それゆえGは3次巡環を含み，そして4重可移性よりすべての3次巡環を含む．したがってGはA_{10}を含む．

11文字の上でGは位数 $11\cdot10\cdot9\cdot8m$ であり，そしてmが奇数であるという仮定なしに4文字を固定する Sylow 部分群の正規化群を考えることによって，$m=1$ でなければならない．3文字を固定する位数8の群は位数2の元を唯一つ含むから，巡回群か四元数群である．巡回群は4元群を自己同型にもつので残りの3文字上3重可移の正規化群をもたない．なぜならばGが3次巡環を含むことになるからである．それゆえ3文字を固定する部分群は四元数群Qである．したがってGはQの可移拡大である．そして T.C. Holyoke [1] の方法によってQから，11文字上の4重可移 Mathieu 群のみならず12文字上の5重可移群をつくることが可能になる．

$t>1$ ならばHが奇数位数であるという仮定に矛盾することを示してこの定理の証明を完成させよう．もし w, x, y, z がVの他の可移成分ならば (5.8.5) より

$$a_2u=(12)(36)(45)(7)(hi)(j)(k)\cdots$$

そして，他の元

$$a_2u'=(12)(36)(45)(7)(wx)(y)(z)\cdots.$$

が存在する．これらの元は a_1 と可換で，a_2 を a_3 にそして a_3 を a_2 に変換する．これらの元の積ははじめの6文字（または7文字）を固定する元qで，奇数位数である．また q は V と可換である．補題 5.8.1 よりqの巾は a_2u を a_2u' に変換するから，a_2u の固定する文字 j, k を a_2u' の固定する文字`y, z にうつす．Vを中心化するので，この元は成分 h, i, j, k を w, x, y, z にうつさねばならない．したがってGの中にはじめの6文字（または7文字）を固定し，Vを中心化し，Vの残りの t 個の成分の上に可移に作用する群Cが存在する．Vの一つの成分をそれ自身に移すCの元は奇数位数だから，すべての4文字を固定しなければならない．したがってCの可移成分は (1)(2)(3)(4)(5)(6)(7) T_h, T_i, T_j, T_k で，最後の4個の集合は，Cの異なる成分である．

pを t を割る素数とする．（ここで $t>1$ という仮定を用いている．）PをCの p-Sylow 群とする．するとCの部分群で1文字を固定するものは指数 $t\equiv0 \pmod p$ でこのような Sylow 群を含むことはできないからPは C がうごか

す $4t$ 個の文字をすべてうごかす．P_1 をPを含み，1, 2, 3, 4 を固定する部分群 H の Sylow 部分群とする．すると，この可能性はあとで考えるが，もし P_1 が $4t+3$ 文字上に作用している

$$p=3,\quad t=3^w,\quad n=4t+7$$

の場合でなければ，P_1 はCのうごかす $4t$ 個の文字だけをうごかす．P_1 は $4t$ 個の文字の上に作用しているので，定理 5.7.2 によって，$N_G(P_1)$ は，はじめの 6 文字または 7 文字の上に 4 重可移であるから，これらの文字上の A_6 または A_7 を含む．しかし，はじめの 6 文字または 7 文字をその上に移す部分群は (5.8.5) の元 u を含むがこの元は，これらの文字上の 交代群には含まれない[1]．したがってGの中にはじめの 6 文字または 7 文字上の対称群が含まれる．そして，それゆえはじめの 4 文字を固定し 5 番目の文字と 6 番目の文字を交換する元を含む．これはHが奇数位数という仮定に反する．最後に，

$$t=3^w,\quad n=4t+7,$$

そしてPがうごかす $4t$ 個の文字と同様に P_1 が 5, 6, 7 をうごかす可能性を考えよう．もし $w>1$ ならば (5, 6, 7) は P_1 の可移成分であり，そしてGの中に元

$$z=(1)(2)(3)(4)(567)\cdots$$

が存在する．$w=1$ ならばPは位数 3 で，元 $(5)(6)(7)(8,9,10)(11,12,13)$ が存在するから 8, 9, 10 を固定する z のような元が存在する．しかし $z=(1)(2)(3)(4)(567)\cdots$ と，(5.8.5) の元 u とで

$$(zu)^3=(1)(2)(35)(4)(6)(7)\cdots,$$

となるが，これは 4 文字を固定する部分群Hが奇数位数という仮定に矛盾する．

Gを 11 文字上の 4 重可移群で S_{11} と A_{11} を除くとする．もしGが (a,b), $(a,b)(c,d)$ または (a,b,c) なる形の元の一つを含むならばGの 4 重可移性によってGはそのような形の元をすべて含むからGは A_{11} または S_{11} でなければならない．Gが 5 次巡環または 7 次巡環を含めば，そのような元はそれのう

1) u ははじめの 6 文字または 7 文字上の奇置換である．

ごかす文字上の可移かつ原始群を生成する．この場合，定理 5.6.2 と 5.7.1 によってGは S_{11} または A_{11} である．これらを除外して，4文字を固定する部分群 $V=V_{1234}$ は $2^4\cdot 3^2$ を割る位数である．Vが単位群でないならばVは 2–Sylow 群または 3–Sylow 群を含まねばならない．いずれにせよ，このような Sylow 部分群Pは丁度6文字をうごかさねばならない．定理 5.7.2 よりPの正規化群は残りの5文字上4重可移，そしてPは (3,3)，(4,2)，または (2,2,2) 文字の可移域をもつからGは5次巡環を含むことになりこの場合はすでに除外されていた．したがって残る唯一つの可能性は4文字を固定する部分群が単位群でそしてGは位数 $11\cdot 10\cdot 9\cdot 8$ となる場合である．

3文字 9, 10, 11 を固定する部分群Wが残りの8文字上正則かつ可移である．それは位数8の5個の相異なる群の一つの正則表現である．Wは位数2の元 $x=(1,2)(3,4)(5,6)(7,8)(9)(10)(11)$ を含む．2文字 10, 11 を固定する部分群Hにおいて W と共役なものは9個存在する．そして各々は1文字を固定する．もし，2個の位数2の相異なる元が同じ互換 (i,j) を含むならば，これらの積は単位元と異なりかつたかだか7文字をうごかす．このようなことは起こらない．しかし位数2の各元は4個の互換を含む．そして，$1,\cdots,9$ の $9\cdot 8/2=36$個の互換が存在する．したがって，W は位数2の元を唯一つ含むから位数8の巡回群または四元数群である．しかしWが巡回群であればその正規化群は位数3の元を含む．そしてこれは (9, 10, 11) なので不可能である．ゆえにWは四元数群Qでなければならない．

10と11を固定する部分群Hは位数72であり9個の四元数群を含む．どの2個も単位元でのみ交わる．単位元と残りの8元は位数9の部分群UをつくりHの正規部分群である．Uの単位元以外の8元はQで共役だからUは基本可換群である．

このことからHを置換群としての同型を除いて容易に構成することができる．Uは

$$u=(123)(456)(789)(10)(11),$$
$$v=(147)(258)(369)(10)(11).$$

で生成される．

$H=QU$，ここでQは

$$a=(1)(2437)(5698)(10)(11),$$
$$b=(1)(2539)(4876)(10)(11).$$

で生成され，そして

$$a^2=b^2$$
$$=(1)(23)(47)(59)(68)(10).$$

11を固定する部分群KはHと，2と11を固定し，1と10を交換する元a^2の共役元xとによって生成される．そのような元はGが4重可移だから必ず存在する．あきらかにxはQを正規化する．Hにxをつけ加えることによって，4文字を固定する単位元と異なる一元を生じてはいけない．可能性は

$$x_1=(1,10)(2)(3)(11)(4,5)(6,8)(7,9),$$
$$x_2=(1,10)(2)(3)(11)(4,6)(5,9)(7,8),$$
$$x_3=(1,10)(2)(3)(11)(4,7)(5,6)(8,9).$$

元$(4,5,6)(7,9,8)$はHを正規化する．そしてこれらの三元をこれらの中でうごかすから置換同型においてこれら三元のどの元をつけ加えてもよい．KをHにx_1をつけ加えて得られた群とする．するとGは1と11を交換し2と10を固定するa^2の共役元yをHに添加することによって得られる．ここでyはQを正規化する．そして1と11を固定する部分群をも正規化する．yに対するただ2つの可能性は

$$y_1=(1,11)(2)(3)(10)(4,6)(5,9)(7,8),$$
$$y_2=(1,11)(2)(3)(10)(4,7)(5,6)(8,9).$$

である．ここで元$(4,9)(5,7)(6,8)$はKを正規化しy_1とy_2を交換する．したがって置換同型においてGはKにy_iを添加して得られると仮定してよい．$G=\{H,x_1,y_1\}$．正確にいえば，11文字上の4重可移群でA_{11}またはS_{11}でないものが存在すればGと置換群として同型になる．Gがこれらの性質を満たすことは演習問題4で与えられる．Gは11文字上の Mathieu 群M_{11}として知られている．注目すべきことは，M_{11}を12を固定する12文字上の置換群と

みなし，そして $M_{12}=\{M_{11}, z\}$,

$$z=(1,12)(2)(3)(10)(11)(4,7)(5,6)(8,9),$$

とすれば M_{12} は位数 $12\cdot 11\cdot 10\cdot 9\cdot 8$ の5重可移群で M_{11} を文字12を固定する部分群として含む.

M_{11} をつくるときに用いたのと同じ方法によって35文字より少ない文字上の4重可移群で交代群または対称群でないものは M_{11}, M_{12}, 23と24文字上の Mathieu 群 M_{23}, M_{24} しか存在しない．ここでもし

$$A=(0,1,2,3,\cdots,22)$$

$$B=(2,16,9,6,8)(4,3,12,13,18),$$
$$(10,11,22,7,17)(20,15,14,19,21).$$

$$C=(0,23)(1,22)(2,11)(3,15)(4,17),$$
$$(5,9)(6,19)(7,13)(8,20)(10,16),$$
$$(12,21)(18,14),$$

とすれば $M_{23}=\{A,B\}$, $M_{24}=\{A,B,C\}$. M_{23} は23次の4重可移群で位数 $3\cdot 22\cdot 21\cdot 20\cdot 16\cdot 3$ であり，M_{24} は5重可移群で文字24を固定する部分群として M_{23} を含む.

5.9. レス積. 対称群の Sylow 部分群

GとHを各々集合AとBの上の置換とする．GのHによる**レス積**（wreath product）$G\wr H$ を次の方法で定義する．すなわち，$G\wr H$ は $A\times B$ 上のすべての置換θからなる次のような群である.

(5.9.1) $$(a,b)\theta=(a\gamma_b, b\eta),\ a\in A,\ b\in B,$$

ここで各 $b\in B$ に対して γ_b はA上のGの置換である．しかし，異なるbに対して置換 γ_b の選び方は独立している．置換ηはB上のHの置換である．$\eta=1$ のとき置換θは正規部分群 G^* を形成し，これはGのn項の直積と同型である．nはBの濃度である．剰余群 $G\wr H/G^*$ はHと同型である．そして，すべての $\gamma_b=1$ のとき置換θはHと同型な部分群をなし，その元はGにおける G^* の剰余類の代表元として取ることができる.

レス積は次の意味で結合律を満たす．もしKが集合C上の第三の置換群とすると，$(G\wr H)\wr K$ と $G\wr(H\wr K)$ は同型で，そしてもし集合 $(A\times B)\times C$ と $A\times(B\times C)$ を $A\times B\times C$ と同一視するならばこれらは等しい．

対称群 S_n の Sylow 部分群はレス積によって容易につくることができる．$n!$ を割るpの最高巾は何か？ pで割れる $n!$ の約数は $p, 2p, 3p, \cdots, kp$, ここで $k=[n/p]$ は n/p をこえない最大の整数である．したがって $n!$ は p^k と $k!$ を割るpの巾で割れる．$[k/p]=[n/p^2]$ に注意しよう．そして $n!$ を割るpの巾が p^M であることをみつける．

$$M=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots.$$

nをpの巾であらわすならば

(5.9.2) $$n=a_0p^u+a_1p^{u-1}+\cdots+a_{u-1}p+a_u,$$

ここで各 a_i は $0\leq a_1\leq p-1$ である．

(5.9.3) $$M=a_0(p^{u-1}+p^{u-2}+\cdots+p+1)+a_1(p^{u-2}+\cdots+p+1)+\cdots+a_{u-1}.$$

特に，p^r 個の元の上の対称群の Sylow 部分群は位数 p^{N_r} で $N_r=p^{r-1}+p^{r-2}+\cdots+1$ である．したがって $p, p^2, \cdots, p^u$ 文字上の対称群の Sylow 部分群ができれば，(5,9,2) で与えられたnに対する対称群の Sylow 部分群を容易に構成することができる．我々はn個の文字を p^u 個の文字からなる a_0 個の組に，p^{u-1} 個の文字からなる a_1 個の組に，…，p 個の文字からなる a_{u-1} 個の組に，そして a_u 個の一文字からなる組に分ける．各組においてSylow 部分群を構成し，そしてこれらの直積をつくれば，位数 p^M の群Pが得られる．M は (5.9.3) で与えられたものである．したがってPは S_n の Sylow 部分群である．

$1, 2, \cdots, p$ 上の S_p の Sylow 部分群は位数pである．そこで Sylow 部分群は $a_1=(1, 2, \cdots, p)$ で生成された位数pの巡回群である．$1, 2, \cdots, p^2$ 上の S_{p^2} は $a_1=(1, 2, \cdots, p)$, $a_2=(p+1,\ p+2, \cdots, 2p), \cdots,$ $a_p=(p^2-p+1, \cdots, p^2)$ で生成された巡回群の直積を部分群に持つ．さらに元 $b=(1, p+1,\ 2p+1, \cdots, p^2-p+1)(2, p+2, \cdots), \cdots, (p, 2p, \cdots, p^2)$, をとれば $b^{-1}a_ib=a_{i+1}$ となる．こ

こで添数はpを法として考える．したがってbと$a_1, \cdots, a_p$は位数p^{p+1}の群P_2を生成する．これはbの第一の巡環と巡回群$\{a_1\}$とのレス積である．P_2はS_{p^2}の Sylow 部分群である．一般にP_rを$1, \cdots, p^r$上のS_{p^r}の Sylow 部分群とする．$S_{p^{r+1}}$の作用する文字として，$1, \cdots, p^r, p^r+1, \cdots, 2p^r, \cdots, p^{r+1}$をとる．そして元

$$c=[1, p^r+1, 2p^r+1, \cdots, (p-1)p^r+1]\cdots$$
$$[j, p^r+j, \cdots, (p-1)p^r+j]\cdots,$$

をとる．ここでjは1から$-p^r$までうごく．すると$P_r^{(i)}=c^{-i}P_rc^i$は文字$ip^r+1, \cdots,$ $(i+1)p^r$上の位数p^{N_r}の群である．各$P_r^{(i)}$，$i=0, 1, \cdots, p-1$，は異なる文字の集合をうごかすからこれらが生成する群はこれらの直積である．ここでcとP_rは位数p^{pN_r+1}の群を生成する．しかし$pN_r+1=p[p^{r-}{}_1+\cdots+(p+1)]+1=N_{r+1}$，より$c$と$P_r$は$p^{r+1}$文字上の対称群の Sylow 部分群$P_{r+1}$を生成する．$P_r$は文字$1, \cdots, p^r$上に作用し，$c$として$c=(u_0, u_1, \cdots u_{p-1})$をとればレス積$P_r \wr \{c\}$は文字$(i, u_j)$，$i=1, \cdots, p^r$，$j=0, \cdots, p-1$，を置換する．もし$(i, u_j)$を$i+jp^r$と同一視するならば，いま定義した$P_{r+1}$はまさにレス積$P_r \wr \{c\}$である．$P_r$は位数$p$の$r$個の元で生成される．

例として，S_8の 2-Sylow 部分群は位数2^7で次の元によって生成されている．

$$a_1=(1, 2),$$
$$b_1=(1, 3)(2, 4),$$
$$c_1=(1, 5)(2, 6)(3, 7)(4, 8).$$

演 習 問 題

1. 無限群Gが有限指数の部分群Hを持つとする．このとき，Hの真の部分群KでG中正規部分群となりかつGにおいて有限指数となるものが存在することを証明せよ．（ヒント：GをHの剰余類上の置換群として表現せよ.）
2. 位数60のただ一つの単純群，5次交代群，が存在することを証明せよ．
3. S_4は6文字上の2個の可移表現をもつことを証明せよ．この2つは忠実ではあるが

置換として同一でないことを示せ.

4. $u=(1,2,3)(4,5,6)(7,8,9)$,
$a=(2,4,3,7)(5,6,9,8)$,
$b=(2,5,3,9)(4,8,7,6)$,
$x=(1,10)(4,5)(6,8)(7,9)$,
$y=(1,11)(4,6)(5,9)(7,8)$,
$z=(1,12)(4,7)(5,6)(8,9)$.
$\{u, a, b, x, y\}$ は Mathieu 群 M_{11} で次数11の4重可移群で位数11・10・9・8であることを示せ. さらに, $\{M_{11}, z\}$ は Mathieu 群 M_{12} で5重可移群であることを示せ. M_{11} は M_{12} の部分群で12を固定することを示せ.

5. $a=(0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22)$,
$b=(2,16,9,6,8)(3,12,13,18,4)(7,17,10,11,22)(14,19,21,20,15)$,
$c=(0,23)(1,22)(2,11)(3,15)(4,17)(5,9)(6,19)(7,13)(8,20)(10,16)(12,21)$
$(14,18)$.
$\{a, b\}$ は次数23の4重可移な Mathieu 群 M_{23} で位数23・22・21・20・16・3であることを示せ. $M_{24}=\{a, b, c\}$ は5重可移 Mathieu 群で, M_{23} は文字24を固定する部分群であることを示せ.

第6章　自　己　同　型

6.1. 代数系の自己同型

任意の集合からそれ自身の上への一対一写像の全体が群をなすことは§1.2でみた．一般に集合Sからそれ自身の上への一対一写像で，ある性質Pを満たすもの全体も群をなす．

Aを一般の代数系で，$X=\{x\}$を元に，そしてAの元 $x_1, \cdots, x_n$ に対し常にAの元yが定まり $f_\mu(x_1, \cdots, x_n)=y$ となるような作用 f_μ を持つとしよう．任意に多くの作用がありうるが，どの作用も n 個の有限個の元の一価函数とする．またAの“法則”および“公理”は作用を含んだ関係である．さて，Xからそれ自身の上への一対一写像$\alpha: X \leftrightarrows X^\alpha$が$A$の**自己同型**(automorphism)であるとは

$$(6.1.1)\qquad f_\mu(x_1, \cdots, x_n)=y \quad ならば \quad f_\mu({x_1}^\alpha, \cdots, {x_n}^\alpha)=y^\alpha$$

が全ての作用 f_μ と，全てのXの元 $x_1, \cdots, x_n$ に対して成立することである．二つの自己同型の積は再び自己同型となり，この積によって自己同型全体は群をなす．したがって特に群の自己同型全体も群をなす．乗法という二元の間の結合が群におけるただ一の作用であるから，一対一写像αが自己同型であるには，$ab=c$ ならば $a^\alpha b^\alpha=c^\alpha$ なることが，あるいはもっと簡単に $(ab)^\alpha=a^\alpha b^\alpha$ が成立することが要求される．

群は，その発生の源を代数系の自己同型にもち，群論の発展は歴史的には代数体の自己同型を研究することから得られたのである．

6.2. 群の自己同型と内部自己同型

群Gからそれ自身の上への一対一写像 $\alpha: x \leftrightarrows x^\alpha$ が自己同型となるための

必要十分条件は $ab=c$ ならば $a^\alpha b^\alpha=c^\alpha$ なることが，あるいはより簡単に

(6.2.1) $$(ab)^\alpha=a^\alpha b^\alpha$$

が成立することである．(6.2.1) だけでは自己準同型なることしか意味しないが，§2.4において すでに一対一自己準同型として自己同型を定義した．したがって群の自己同型に関する二つの定義は一致する．

Gの元aを固定したとき

(6.2.2) $$A_a : x \leftrightarrows a^{-1}xa, \quad \forall x \in G$$

なる写像 A_a は，$axa^{-1} \to a^{-1}(axa^{-1})a=x$ ゆえ一対一であり，また $a^{-1}xya =a^{-1}xa\cdot a^{-1}ya$ が成り立つから自己同型である．(6.2.2) で定義されたGの自己同型 A_a を**内部自己同型** (inner automorphism) という．内部自己同型でないGの自己同型を**外部自己同型** (outer automorphism) という．

$b^{-1}(a^{-1}xa)b=(ab)^{-1}x(ab)$ および $a(a^{-1}xa)a^{-1}=x$ から

(6.2.3) $$A_aA_b=A_{ab}\ , \quad A_{a^{-1}}=A_a{}^{-1}$$

が成り立つ．

定理 6.2.1. 群Gの内部自己同型全体 $I(G)$ はGの自己同型全体のなす群 $A(G)$ の正規部分群をなし，写像 $a \to A_a$ はGから $I(G)$ の上への準同型でその核はGの中心に一致する．

証：(6.2.3) により $I(G)$ は $A(G)$ の部分群である．α をGの任意の自己同型とすると $(a^{-1}xa)^\alpha=(a^\alpha)^{-1}x^\alpha a^\alpha$ から $\alpha^{-1}A_a\alpha : x\to(a^\alpha)^{-1}xa^\alpha$ が，したがって $\alpha^{-1}(A_a)\alpha=A_{a^\alpha}$ が成り立ち $I(G)$ は $A(G)$ の正規部分群となる．また(6.2.3) は写像 $a\to A_a$ がGから $I(G)$ の上への準同型なることを示している．さて $A_a=1$ はGの全ての元xに対し $xa=ax$ なるとき，しかもそのときに限るから準同型 $G\to I(G)$ の核はGの中心となる．

有限可換群Xは Sylow 部分群の直積となっている (定理 3.2.3).

(6.2.4) $$X=S(p_1)\times S(p_2)\times\cdots\times S(p_r)$$

Xの自己同型群 $A(X)$ は自己同型群 $A[S(p_i)]$ の直積を含まねばならないが，Xの自己同型は $S(p_i)$, $i=1\cdots r$ をそれ自身の上に写すことから $A[S(p_i)]$

の直積に含まれる．したがって次のことが成り立つ．

(6.2.5) $$A(X)=A[S(p_i)]\times\cdots\times A[S(p_r)]$$

さらに一般に可換周期群の自己同型群は Sylow 部分群の自己同型群の Cartesian 積となる．

したがって可換周期群の自己同型を求めるには，可換 p 群の自己同型を求めることに帰着される．有限可換 p 群 A_p のどの自己同型も基底を基底に写す．逆に $a_1, \cdots, a_s$ と $b_1, \cdots, b_s$ を A_p 二つの基底で定理 3.3.2 におけると同じ順序で並んでいる，すなわち a_i と b_i $(i=1, \cdots, s)$ が同じ位数を持つとすると，

(6.2.6) $$\begin{aligned} A_p &= \{a_1\}\times\{a_2\}\times\cdots\times\{a_s\} \\ &= \{b_1\}\times\{b_2\}\times\cdots\times\{b_s\} \end{aligned}$$

であるから

(6.2.7) $$a_i \to (a_i)\alpha = b_i \quad i=1, \cdots, s$$

なる写像は A_p の自己同型 α を定める．

位数が p の巡回群 $C=\{a\}$, $a^p=1$ においては $a^i, i=1, \cdots, p-1$ は生成元であるから $a\to(a)\alpha_i=a^i$ により定まる $p-1$ 個の自己同型がある．さて r を mod. p の原始根*) とすると，$a\to(a)\beta=a^r$ は自己同型 β を定める．このとき $a\to(a)\beta^j=a^{r^j}$ であって，$r^j\equiv1$ (mod. p) となる j の最小値は $p-1$ である．したがって自己同型 β の位数は $p-1$ となり自己同型群 $A(C)$ は β で生成される位数 $p-1$ の巡回群である．

6.3. 群のホロモルフ

群 G の左正則表現全体および右正則表現全体はともに G の元の置換全体が作る群 S_G の部分群をなす (§ 1.4)．また α を G の自己同型とすると，$\alpha: x \leftrightarrows x^\alpha$ は G の単位元 1 をうごかさない S_G の元である．

$(g_1x)g_2=g_1(xg_2)$ であるから，$L(g_1)R(g_2)=R(g_2)L(g_1)$ が成り立ち，した

*) 原始根の取り扱いについては，Birkhoff and MacLane [1] p. 446 か Hardy and Wright [1] p. 236 を参照．

がって，Gの左右正則表現は元ごとに可換である．

定理 6.3.1. Gの左正則表現全体および右正則表現全体は，それぞれ一方が他方の S_G の中での中心化群に等しい．

証：π を $L(G)$ の中心化群に属する S_G の元とし，$(1)\pi=g$ とする．このとき $\pi R(g)^{-1}=\pi^*$ は $L(G)$ の中心化群の元で単位元1をうごかさない．したがって $(1)\pi^*L(g')=g'$ が成り立つから $(1)L(g')\pi^*=g'$ も成り立ち，したがって $(g')\pi^*=g'$ が得られる．しかるに g' はGの任意の元であったから $\pi^*=1$ となり，$\pi\in R(G)$ をうる．したがって $L(G)$ の中心化群は $R(G)$ に等しくなる．同様にして $L(G)$ が $R(G)$ の中心化群に一致することがいえる．

これで $R(G)$ の S_G の中での中心化群が分かった．S_G の中での $R(G)$ の正規化群をGの**ホロモルフ**という．

定理 6.3.2. Hを群Gのホロモルフすなわち S_G の中での $R(G)$ の正規化群とすると，Gの単位元を固定するHの部分群はGの自己同型群 $A(G)$ になる．

証：$R(G)$ の正規化群をH，α を1をうごかさないHの元とすると $R(G)$ がHの正規部分群なることから $R(g)\leftrightarrows\alpha^{-1}R(g)\alpha$ は $R(G)$ の自己同型となる．したがって $\alpha^{-1}R(g)\alpha=R(g^\alpha)$ と置くと，これによりGからそれ自身の上への一対一写像が定まるが，この写像により・$(g_1g_2)^\alpha=g_1{}^\alpha g_2{}^\alpha$ が成り立つから $g\leftrightarrows g^\alpha$ はGの自己同型となる．また $(1)\alpha=1$，$\alpha^{-1}R(g)\alpha=R(g^\alpha)$ から，$(1)\alpha R(g^\alpha)=g^\alpha$，$(1)R(g)\alpha=g^\alpha$ が，したがって $(g)\alpha=g^\alpha$ が成り立つことになる．ゆえに α はGの自己同型である．逆に $\alpha: g\leftrightarrows g^\alpha$ をGの自己同型とすると，α はGの単位元1をうごかさない S_G の元である．このとき $\alpha^{-1}R(g)\alpha=R(g^\alpha)$ なることを示せば α は $R(G)$ の正規化群に含まれることになる．$(x)R(g)\alpha=x^\alpha g^\alpha$ および $(x)\alpha R(g^\alpha)=x^\alpha g^\alpha$ なることから $\alpha^{-1}R(g)\alpha=R(g^\alpha)$ が成り立つ．またある群の正規化群はその中心化群を含むから，$H\supset L(G)$ が成り立つ．

6.4. 完　備　群

定　義：中心が単位元のみからなる群で，自己同型がすべて内部自己同型である群を**完備群**（complete group）という．

定理 6.4.1. 群Tの正規部分群Gが完備群であれば，GのT中の中心化群をKとすると，$T=K\times G$ となる．

証：Tを次のように分解する．

(6.4.1)
$$T=G+Gx_2+\cdots+Gx_i+\cdots$$

GはTの正規部分群ゆえ $x_i^{-1}Gx_i=G$ が成り立つから $g\leftrightarrows x_i^{-1}gx_i=g^{\alpha}$ はGの自己同型である．Gの自己同型はすべて内部自己同型であるからGのある元 a と任意の元gに対して $g^{\alpha}=a^{-1}ga$ が成り立つ．したがって $x_i^{-1}gx_i=a^{-1}ga$ が成り立ち $y_i=x_ia^{-1}$ はTの中でのGの中心化群Kの元となる．しかるに $Gx_i=x_iG=x_ia^{-1}G=y_iG=Gy_i$ から y_i をGによるTの剰余類の代表に取ることができる．したがってどの剰余類もKの元を含むことになり，かつGはT中正規ゆえ $T=G\cup K=GK=KG$ が成り立つ．一方Gの中心は単位元のみからなるから $K\cap G=1$ となり，したがって $T=K\times G$ が成り立つ．

系 6.4.1. 完備群GのホロモルフHは $R(G)$ と $L(G)$ の直積 $R(G)\times L(G)$ に等しい．

$L(G)$ がHの中での $R(G)$ の中心化群なることから明らかである．

6.5. 正規積または半直積

定理 6.5.1. 二つの群 H, K とHの各元hに対しKの自己同型

(6.5.1)
$$k\leftrightarrows k^h,\quad \forall k\in K$$

で

(6.5.2)
$$(k^{h_1})^{h_2}=k^{h_1h_2},\quad h_1, h_2\in H$$

を満たすものが与えられたとする．このとき記号 $[h, k]$ $(h\in H,\ k\in K)$ に対

し乗法を

$$[h_1, k_1]\cdot[h_2, k_2]=[h_1h_2, k_1{}^{h_2}k_2] \tag{6.5.3}$$

により定義すれば一つの群が得られる．この群をHによるKの正規積または半直積という．

証：まずすべての k, h に対し $k^h\in K$ が成り立つから (6.5.3) で乗法を定義することは可能である．

1） (6.5.3) の乗法は結合律を満たす．

$$\begin{aligned}&([h_1, k_1]\cdot[h_2, k_2])\cdot[h_3, k_3]\\&=[h_1h_2, k_1{}^{h_2}k_2]\cdot[h_3, k_3]\\&=[(h_1h_2)h_3, (k_1{}^{h_2}k_2)^{h_3}k_3]\\&=[h_1h_2h_3, k_1{}^{h_2h_3}k_2{}^{h_3}k_3]\end{aligned} \tag{6.5.4}$$

一方 (6.5.1), (6.5.2) を使うと

$$\begin{aligned}&[h_1, k_1]\cdot([h_2, k_2]\cdot[h_3, k_3])\\&=[h_1, k_1]\cdot[h_2h_3, k_2{}^{h_3}k_3]\\&=[h_1h_2h_3, k_1{}^{h_2h_3}k_2{}^{h_3}k_3]\end{aligned} \tag{6.5.5}$$

が得られて結合律が成り立つ．

2） 元 [1, 1] が単位元となる．

$$[1, 1]\cdot[h, k]=[1h, 1^hk]=[h, k],$$

$$[h, k]\cdot[1, 1]=[h1, k^11]=[h, k]$$

(6.5.2) から $k^1=k$ が得られるからである．

3） 任意の元 $[h, k]$ の左逆元は $[h^{-1}, (k^{-1})^{h^{-1}}]$ である．

$$[h^{-1}, (k^{-1})^{h^{-1}}]\cdot[h, k]=[h^{-1}h, k^{-1}k]=[1, 1] \tag{6.5.6}$$

が成り立つからである．

以上から (6.5.3) の乗法により $[h, k]$ 全体は群をなす．

定理 6.5.2. GをHによるKの半直積とすると，Gの $[h, 1]$ なる元全体はHに同型な部分群を，また $[1, k]$ なる元全体はKに同型な正規部分群をそれぞれなす．さらにKをGの部分群とみたときKの自己同型 (6.5.1) は

$$[h,1]^{-1}\cdot[1,k]\cdot[h,1]=[1,k^h] \tag{6.5.7}$$

によりGの部分群とみたときのHの元 $h=[h,1]$ による変換により引き起こされる．また

$$[h,1]\cdot[1,k]=[h,k] \tag{6.5.8}$$

から $G=H\cup K$ が成り立つ．

証：(6.5.3) と $k^1=k$ なることを使うと $h\leftrightarrows[h,1]$, $k\leftrightarrows[1,k]$ がそれぞれ H,K とGの部分群の間の同型を与えることが分かり前半が示されたことになる．また (6.5.3) から直ちに (6.5.7), (6.5.8) が得られ (6.5.7) はKがGの（部分群とみたとき）正規部分群なることおよび自己同型 (6.5.1) が $h=[h,1]$ による変換により引き起こされることを示している．$H\cap K=[1,1]=1$ であるから (6.5.8) はKによるGの剰余類の代表元にHの元が取れることを示している．

定理 6.5.3. GがHによるKの半直積であるための必要十分条件は，KがGの正規部分群，HがGの部分群でKによるGの剰余類の代表元にHの元が取れることである．これは換言すれば次のようになる．

1) KはGの正規部分群である．
2) HはGの部分群である．
3) $H\cap K=1$.
4) $K\cup H=G$.

証：GがHによるKの半直積であれば 1)〜4) が成り立つことはすでに述べた．逆に 1)〜4) が成り立つとしよう．このとき 1), 3), 4) からGの各元は一意的に

$$g=hk \tag{6.5.9}$$

と表わされる（定理 2.3.3)．Kが正規部分群であるから

$$h^{-1}kh=k^h\in K \tag{6.5.10}$$

が成り立ち，$k\leftrightarrows k^h$ は明らかにKの自己同型となる．また (6.5.10) から

(6.5.11)
$$(k^{h_1})^{h_2}=k^{h_1h_2}$$

が成り立つ．Gの二元の間の積に対しては，

$$g_1=h_1k_1,\quad g_2=h_2k_2,$$

(6.5.12)
$$\begin{aligned}g_1g_2&=h_1k_1h_2k_2\\&=h_1h_2(h_2^{-1}k_1h_2)k_2\\&=h_1h_2\cdot k_1^{h_2}k_2,\end{aligned}$$

が成り立つから，Gにおける乗法は (6.5.3) の法則と一致することになり，したがってGはHによるKの半直積となる．

Hの元はKの自己同型を引き起こすから，HからKの自己同型群の中への準同型が定義される．もしこの準同型によりHがKの自己同型群の単位元に写される．すなわち $k^h=k$ がすべての k,h に対して成立するとすれば，(6.5.3) はHとKとの直積に対する乗法則となる．

演　習　問　題

1. 位数8の二面体群はその自己同型群に同型なることを示せ．
2. 位数 p^r の基本可換群の自己同型群は $(p^r-1)(p^r-p)\cdots(p^r-p^{r-1})$ の位数を持つ．
3. 6次の対称群 S_6 の外部自己同型を求めよ．この自己同型は位数3の元からなる二つの共役類を互いに入れ換える．
4. p を素数として，群の位数が p^2 で割り切れるならばその群の自己同型群の位数は p で割り切れることを示せ．
5. 群Gの自己同型αは，Gの中心をZとしGの各元xに対し $x^{-1}(x)\alpha\in Z$ を満たすとき，中心自己同型と呼ばれる．Gの内部自己同型であって中心自己同型なるもの全体が作る群は G/Z の中心に同型なることを示せ．
6. Gを $a^8=b^8=c^4=1$，$b^{-1}ab=a^5$，$c^{-1}ac=a^5$，$c^{-1}bc=a^6b$ なる関係式をもつ元 a,b,c で生成された群とする．このとき $\{a,b\}$ は $\{b\}$ による $\{a\}$ の半直積なることおよびGが $\{c\}$ による $\{a,b\}$ の半直積なることを示せ．このことから上の関係式は $a^ib^jc^k$ なるかたちの元からなる位数256の群を定義する．

第7章　自　由　群

7.1. 自由群の定義

$s_1, \cdots, s_n$ を元に持つ集合 S が与えられたとする．ここに $s_1, \cdots, s_n$ が有限個であるとか可算個であるとかは仮定しない．しかし必要なときには s_i の添数 i の集合が整列集合なることは仮定する．$s_i^1 = s_i$，s_i^{-1} を新しい記号として s_i^1, s_i^{-1} を定義する．

a_i を s_j^ϵ，$\epsilon = \pm 1$，のいずれか一方とし有限列 $a_1a_2\cdots a_t$ と 1（このような列がないとき 1 とかく）を**語**（word）という．

語が 1 に等しいか，$a_1\cdots a_t$ であってどの a_ia_{i+1}，$i=1, \cdots, t-1$，も $s_j^\epsilon s_j^{-\epsilon}$，$\epsilon = \pm 1$，なる型でないとき**簡約された語**（reduced word）であるという．

二つの語 f_1, f_2 が $f_1 = gs_j^\epsilon s_j^{-\epsilon}h$，$f_2 = gh$ とかけているとき**隣り合っている**（adjacent）という．このとき f_1, f_2 のいずれか一方は他方に**隣り合っている**という．

二つの語 f, g が，$f \sim g$ とかいて**同値**であるとよぶのは f_i, f_{i+1}（$i=1, \cdots, m-1$）なる隣り合った語が存在して $f_1 = f$，$f_2, \cdots$，$f_m = g$ となるときである．定義から明らかに $f \sim g$ は語の集合における同値関係となる．この同値関係により語を分類したとき f が属する類を $[f]$ で表わすことにする．

補題 7.1.1. どの類も一つしかもただ一つだけ簡約された語を含む．

証：$f = a_1\cdots a_t$ においてもし $a_ia_{i+1} = s_j^\epsilon s_j^{-\epsilon}$ となっていれば f と隣り合った語で f よりも少ない記号で表わされる語 $a_1\cdots a_{i-1}a_{i+2}\cdots a_t$ が存在する．このような簡約を引き続いて行なうとたかだか $t/2$ 回の操作により f に同値であって簡約された語を求めることができる．したがって $[f]$ は少なくとも一つ簡約された語を含む．

さて $f=a_1\cdots a_t$ に対してW過程なるものを次のように定義する.

$$W_0=1 \qquad f=1$$
$$W_1=a_1$$
$$W_{i+1}=W_ia_{i+1}：もし W_i が Xa_{i+1}^{-1} なる形の既約形でないとき$$
$$=X \qquad ：もし W_i が Xa_{i+1}^{-1} なる形の既約形のとき$$

帰納的に $W_0, W_1, \cdots, W_t$ が既約形であることおよび f が既約形であれば $W_t=f$ が成立することが示される. また

$$f_1=a_1\cdots a_ra_{r+1}\cdots a_t,$$
$$f_2=a_1\cdots a_rs_j^{\epsilon}s_j^{-\epsilon}a_{r+1}\cdots a_t,$$

とし f_1, f_2 に対するW過程により得えらる語をそれぞれ $W_0^1, W_1^1, \cdots, W_t^1, W_0^2, W_1^2, \cdots, W_{t+2}^2$ とすると $W_t^1=W_{t+2}^2$ なることを示そう. まず作り方から $W_0^1=W_0^2, \cdots, W_r^1=W_r^2$ が成り立つことはよい. そこで次の二つの場合に分けて考える.

1)　$W_r^1=W_r^2$ が $Xs_j^{-\epsilon}$ なる形の既約形である. $Xs_j^{-\epsilon}$ が既約であるから Xは Ys_j^{ϵ} なる形の既約形ではない. したがって f_2 に対しては $W_{r+1}^2=X$, $W_{r+2}^2=Xs_j^{-\epsilon}=W_r^2=W_r^1$ が成り立つ.

2)　$W_r^1=W_r^2$ が $Xs_j^{-\epsilon}$ なる形の既約形でない. このときは $W_{r+1}^2=W_r^2s_j^{\epsilon}$, $W_{r+2}^2=W_r^2=W_r^1$ が成り立つ.

したがっていずれの場合も $W_{r+2}^2=W_r^1$ が成立し以下帰納的に $W_{r+2+i}^2=W_{r+i}^1$ なることが示される. したがってW過程によりどの二つの隣り合った語からもしたがってどんな二つの同値な語からも同じ既約語が得られる. ゆえに同じ類には異なる既約語は含まれない.

これら同値類の間に乗法が定義されこの乗法により同値類全体が群をなす. この群をSにより生成された自由群Fという.

定理 7.1.1. S上の語のどの二つの類 $[f_1]$, $[f_2]$ に対しても $[f_1][f_2]=[f_1f_2]$ によって乗法を定義すれば, まずこの乗法は定義可能であってこの乗法によりS上の語の類全体は群をなす. この群をSで生成された自由群Fという.

証：$f_1 \sim f_1'$, $f_2 \sim f_2'$ とすると f_1f_2 において f_1 をそれと隣り合った語で順次置き換えていっても同値であるから $f_1f_2 \sim f_1'f_2$ が成り立つ．同様にして $f_1'f_2 \sim f_1'f_2'$ が成り立つから $f_1f_2 \sim f_1'f_2'$ が成り立ち，したがって $[f_1'f_2'] = [f_1f_2]$ が成立する．これから乗法 $[f_1f_2]=[f_1][f_2]$ は f_1 および f_2 が属する類によってのみ定まりそれらの類の代表元の取り方には関係しない．また $[1][f]=[f][1]=[f]$ から $[1]$ がこの乗法の単位元となる．また $f=a_1\cdots a_t$ のとき $h=a_t^{-1}\cdots a_1^{-1}$ と置くと $[f][h]=[fh]=[1]$, $[h][f]=[hf]=[1]$ が成り立つから $[a_1\cdots a_t]$ の逆元は $[a_t^{-1}\cdots a_1^{-1}]$ であり $([f_1][f_2])[f_3]=[f_1f_2f_3]=[f_1]([f_2][f_3])$ から結合律も成り立つ．以上から同値類全体は群をなす．この群を生成元を示すため F_S とかくこともある．

二つの語 f_1, f_2 が同値であるすなわちFの同じ元を表わすとき便宜上 $f_1 = f_2$ とかく．また f_1, f_2 が同一語を表わすことを示すのに $f_1 \equiv f_2$ とかくことにする．当然のことながらFの元は既約形で代表させるのが便利であろう．そこで $f=a_1\cdots a_t$ が既約形であるときfは既約に表わされているということにする．

群においては $x_1, \cdots, x_m$ なる元の集合Xは，b_j を x_j^ϵ, $\epsilon=\pm 1$, としたとき $b_1b_2\cdots b_t$ なる形の有限個の積全体からなる部分群Hを生成する．このような有限個の積全体が部分群をなすことは容易に示される．一般にHの元を有限個の積として表わすのに幾通りもの表わし方がある．またGの元全体は明らかにGを生成するからどの群Gもある元の集合Xにより生成されるとみられる．このとき $G=\{X\}$ とかくことにする．次の定理は自由群がそれ自体興味あるだけでなくあらゆる群を研究するに当って有効な手段となることを示している．

定理 7.1.2. 元の集合 $X : x_1, \cdots, x_n$, により生成された群をGとする．このときもしFを $S : s_1, \cdots, s_n$, で生成された自由群とすると $s_i \to x_i$ $(i=1, \cdots, n)$ により定まる準同型 $F \to G$ が存在する．

証：$f=a_1\cdots a_t$ をS（上）の任意の語としたとき $a_i = s_j^\epsilon$ なら $b_j = x_j^\epsilon$ と置いてGの元 $g=b_1\cdots b_t$ を考える．このとき $f \to g$ によってSの各語はGの元

に写される．Sの隣り合った語すなわち同値な語はGの同じ元に写されるのは明らかであるから $f \to g$ はFからGの上への写像となる．また $f_1 \to g_1$，$f_2 \to g_2$ であれば $f_1 f_2 \to g_1 g_2$ となり写像 $s_i \to x_i$ はFからGの上への準同型となる．準同型に関する定理から次の系が得られる．

系 7.1.1. 集合Xで生成されるどの群GもXと同じ個数の生成元を持つ自由群Fの剰余群となる(同型である)．

定 義：元の集合Sで生成された自由群Fは次の性質を持った群とする．

1) FはSで生成される．

2) Gを元の集合Xで生成される任意の群としたときSとXとの間に一対一対応 $S \leftrightarrows X$ があればFからGの上への準同型 $F \to G$ でSをXの上に写すものがある．

定理 7.1.2 からこのように定義しても差し支えない．はじめに与えられた自由群 F_S の定義から F_S は上の定義の条件 1)，2) を満たしている．またもし F' をSで生成される群で $F' \to F_S$ とすると F' の元で単位元に写されるのは単位元だけであるからこの準同型は同型でなければならない．

しかしこの定義にはいくつかの不利な点がある．まづ積極的な定義ではないし上に示されたような過程を経て作るのでなければ条件 1)，2) を満たす群が存在するかどうかはっきりしないし，また仮にそのような群が存在したとしても自明でない関係を持つことがないかどうかもはっきりしない．その上もっと広い立場に立ってみると“自由な”系——それは公理による関係を除けばどんな関係もない系のことであるが——をたとえ定理 7.1.2 に類似した定理が成立しないとしても考えることはできるのである．

7.2. 自由群の部分群．Schreier の方法

部分群の性質が群を研究するにあたっての基本となるのが常であって定理 7.1.2 から自由群に対しては正規部分群がとくに興味の対称となる．Nielsen

が [1] でまた Schreier が [3] で自由群の部分群が再び自由群となることを示した. Nielsen の証明は有限生成の部分群についてのみなされたが, この有限生成という制限を取り除くために Levi [1] とか他の人々により Nielsen の証明は拡張されてきた. Nielsen の方法は部分群の元を直接あつかうことであり, Schreier は部分群による剰余類をあつかうという方法をとった. これから示す最初の証明は Schreier の証明を簡単にしたものである*).

自由群 F の元の集合 G が **Schreier 系**であるとは G の各元 g に対して次のことが成り立つときである.

1) $g=a_1a_2\cdots a_t$ が既約に表わされている

2) $a_1a_2\cdots a_{t-1}$ も G の元である.

また 1), 2) に加えて

3) $a_2\cdots a_t$ も G の元である

が成り立つとき G を**両側 Schreier 系**という. 定義から Schreier 系はいつも 1 を含む.

F を S で生成された自由群, U を F の部分群とし F を U による左剰余類に分ける.

(7.2.1)
$$F=U\cdot 1+U\cdot g_2+\cdots+U\cdot g_i+\cdots$$

U の代表元としていつも単位元をとることにする. U 以外の剰余類の代表元としてはある関係を満たすものを選ぶのが好都合である.

補題 7.2.1.（拡張された Schreier の補題） U を自由群 F の部分群とすれば U による左剰余類の代表系に Schreier 系を取ることができる. もし U が F の正規部分群であれば両側 Schreier 系を代表系に取ることができる.

証：F の生成元を $S: s_1, \cdots, s_n,$ とし $S\cup S^{-1}$ に順序を入れて全順序集合とする. たとえば n が有限のときは $s_1<s_1^{-1}<s_2<s_2^{-1}<\cdots<s_n<s_n^{-1}$ というように…. しかし S を有限または可算集合とは仮定せず単に $S\cup S^{-1}$ が全順序集合なることを仮定する.

*) Hall and Rado [1] をみよ. またより以上の結果については M. Hall [4, 5] を参照.

$S \cup S^{-1}$ の順序を拡張してFのすべての元の間に**辞書式順序**を次のように入れることができる．Fの二元 f, g に対して

$$f = a_1 \cdots a_t, \qquad a_i, b_j \in S \cup S^{-1}$$
$$g = b_1 \cdots b_u,$$

を既約形としたとき次の 1)，2)，3) のいずれか一つが成り立つとき辞書式順序で $f < g$ と定義する．

1) $t < u$.

2) $t = u$, $a_1 < b_1$.

3) $t = u$, $a_1 = b_1, \cdots, a_i = b_i$, $a_{i+1} < b_{i+1}$.

上に定義された辞書式順序は全順序であって次の性質を持つ．

$f < g$ であって gh が既約に表わされているならば $fh < gh$ が成り立つ．また $f < g$ であって hg が既約に表わされているならば $hf < hg$ が成り立つ．この証明は定義から明らかであろう．

補題を証明するために剰余類 Ug_i の元の中でFの辞書式順序で最初の元をその剰余類の代表 g_i に選ぶことにする．このとき g_i 全体が Schreier 系をなし，もしUが正規部分群であれば両側 Schreier 系となることを示そう．単位元はFの最初の元であるからUの代表元は単位元である．剰余類 Ug の元の中で最初の元を $g = a_1 \cdots a_{t-1} a_t$ としまた $h^* = a_1 \cdots a_{t-1}$ を含む剰余類の最初の元をhとする．もし $h = b_1 \cdots b_u$ とすると $h \leq a_1 \cdots a_{t-1}$ であって $ha_t \in Ug$ から $g \leq ha_t$ となる．一方 $ha_t \leq a_1 \cdots a_{t-1} a_t = g$ から $g = ha_t$ が成り立ちしたがって $h = h^* = a_1 \cdots a_{t-1}$ も剰余類の代表元である．ゆえに g_i 全体は Schreier 系をなす．Uを正規部分群としfを最初の元とする剰余類 $Uf = fU$ に $a_2 \cdots a_t$ が含まれているとすると，$f \leq a_2 \cdots a_t$ および $a_1 f \in a_1 \cdots a_t U = gU = Ug$ が成り立つから $g \leq a_1 f$ をうる．しかるに $a_1 f \leq a_1 a_2 \cdots a_t = g$ であるから $g = a_1 f$ がしたがって $f = a_2 \cdots a_t$ が成立する．これはg全体が両側 Schreier 系なることを示している．この補題は Schreier 系の存在を示すだけであって同じ部分群に対して剰余類の代表系に二つ以上の Schreier 系をとることも可能である．

主（要）定理：定理 7.2.1. 自由群の部分群は自由群である．

FをSで生成された自由群，UをFの部分群とする．このとき Schreier の補題から左剰余類の代表系Gを Schreier 系に取ることができる．

(7.2.2) $$F=U\cdot 1+U\cdot g_2+\cdots+U\cdot g_i+\cdots$$

自由群であるか否かを問わず任意の群Fに対して成立する補題からはじめよう．FをSで生成される群，UをFの部分群とし (7.2.2) をUによるFの左剰余類への分解とする．もしFの元fが (7.2.2) における剰余類 Ug_i の元であるとき，$\Phi(f)=g_i$ によって函数 $\Phi(f)$ を定義する．このとき $u\in U$ ならば $\Phi(uf)=\Phi(f)$ でありまた $\Phi(f)=1$ と $f\in U$ は同値である．

$S\cup S^{-1}\ni a_i$ に対して $f=a_1a_2\cdots a_t$ であるとき $f_0=1$, $f_1=a_1$, $f_2=a_1a_2,\cdots$, $f_t=a_1\cdots a_t=f$ としまた $h_0=\Phi(f_0)=1$, $h_1=\Phi(f_1),\cdots$, $h_t=\Phi(f)$ と置くと

(7.2.3) $$fh_t^{-1}=h_0a_1h_1^{-1}\cdot h_1a_2h_2^{-1}\cdot h_2\cdots h_{t-1}^{-1}\cdot h_{t-1}a_th_t^{-1}$$

であり，もし $f\in U$ なら $h_t=1$ から

$$=f$$

が成り立つ．

さて $h_i=\Phi(h_i)=\Phi(f_i)=\Phi(f_{i-1}a_i)=\Phi(h_{i-1}a_i)=\Phi(h_{i-1}s_a{}^{\epsilon})$, $a_i=s_a{}^{\epsilon}$, $\epsilon=\pm1$, $h_i\in G$ であるから (7.2.3) から $g\in G$, $s^{\epsilon}\in S\cup S^{-1}$ に対して gs^{ϵ} なる形の元に対してのみ函数 Φ が定義されているものが重要となる．そこで $f=gs^{\epsilon}$ なる元に対してだけ定義された $\phi(f)$ に対して $\phi(gs^{\epsilon})=\Phi(gs^{\epsilon})$ とかくことにする．

補題 7.2.2. 任意の群Fに対して元 $gs\phi(gs)^{-1}$ 全体はUの生成元となる．ただしgは (7.2.2) の剰余類の代表元全体を，またsはFの生成元全体をそれぞれ動き，また $\phi(gs^{\epsilon})$ は gs^{ϵ} を含む剰余類の代表とする．

証：もし $f\in U$ とすると $h_t=1$ であって (7.2.3) からfは $h_{i-1}a_ih_i^{-1}$ の積とかける．また $h_i=\Phi(h_{i-1}a_i)$ であるから $h_{i-1}a_ih_i^{-1}$ は $h_{i-1}=g$, $a_i=s^{\epsilon}$ とすると $gs^{\epsilon}\phi(gs^{\epsilon})^{-1}$ とかける．したがって $h_i=\phi(gs^{\epsilon})$ となる．しかるに $gs^{\epsilon}\in U\cdot\phi(gs^{\epsilon})$ から任意の gs^{ϵ} に対して $gs^{\epsilon}\phi(gs^{\epsilon})^{-1}\in U$ が成り立つ．ここで $\phi(g_js^{\epsilon})=g_k$ とすれば $\phi(g_ks^{\epsilon})=g_j$ なることに注意すれば $g_js^{\epsilon}\phi(g_js^{\epsilon})^{-1}=g_js^{\epsilon}g_k^{-1}$ で

あるとすると，その逆元は $g_k s^{-\epsilon} g_j^{-1} = g_k s^{-\epsilon}\phi(g_k s^{-\epsilon})^{-1}$ となり s の巾の符号をかえただけの形をしている．ゆえに $gs\phi(gs)^{-1}$ はUを生成する．

系 7.2.1. Fを有限生成の群，Uを有限指数のFの部分群とすればUも有限生成となる．

$gs\phi(gs)^{-1}$ において g, s の取り方が有限個であることからこの系は得られる．

これから後はFを自由群とし剰余類の代表系Gが Schreier 系であると仮定する．

函数 $\phi(gs^\epsilon)$ についての次の性質を使うことにする．

1) $\phi(gs^\epsilon)\in G$.

2) もし $\phi(gs^\epsilon)\in G$ であれば $\phi(gs^\epsilon)=gs^\epsilon$.

3) $\phi[\phi(gs^\epsilon)s^{-\epsilon}]=g$.

一般的記号として $v=gs^\epsilon\phi(gs^\epsilon)^{-1}$, $u=gs\phi(gs)^{-1}$ とかくことにする．このとき uは $\epsilon=1$ のときの v であり v は u か u^{-1} に等しい．なぜならば $v=g_i s^{-1}\phi(g_i s^{-1})^{-1}$ とするとき $\phi(g_i s^{-1})=g_j$ と置くと 3) から $v^{-1}=g_j s g_i^{-1}=g_j s\phi(g_j s)^{-1}=u$ となり，同様にして $u^{-1}=v$ も成り立つからである．

補題 7.2.3. $v=gs^\epsilon\phi(gs^\epsilon)^{-1}$ は既約に表わされているか1に等しい．

証：$v=g_j s_a^\epsilon\phi(g_j s_a^\epsilon)^{-1}=g_j s_a^\epsilon g_k^{-1}$, $g_k=\phi(g_j s_a^\epsilon)$ とすると g_j, g_k^{-1} は既約に表わされているからもしvに簡約するところがあれば，（1）g_j が $s_a^{-\epsilon}$ で終る，（2）g_k^{-1} が $s_a^{-\epsilon}$ ではじまる，のいずれかである．もし（1）の場合は $g_j=a_1\cdots a_{t-1}s_a^{-\epsilon}$ が g_j の既約形である．このときは $g_j s_a^\epsilon=a_1\cdots a_{t-1}$ はGの元であるからϕの性質 2) を使うと $g_k=\phi(g_j s_a^\epsilon)=g_j s_a^\epsilon$ が成り立ち，したがって $v=g_j s_a^\epsilon g_k^{-1}=1$ となる．（2）の場合も同様にして $g_j=\phi(g_k s_a^{-\epsilon})=g_k s_a^{-\epsilon}$ から $v=1$ が得られる．

$v=gs^\epsilon\phi(gs^\epsilon)^{-1}\neq 1$ のとき s^ϵ をvの**主要因子** (significant factor) という．$v=g_j s_a^\epsilon\phi(g_j s_a^\epsilon)^{-1}=g_k s_b^\eta\phi(g_k s_b^\eta)^{-1}\neq 1$ とする．もし g_j と g_k が同じ長さであ

れば v は既約に表わされているから $g_j=g_k$, $s_a{}^\epsilon=s_b{}^\eta$ となる. またもし g_j と g_k が異なる長さをもてば, たとえば g_k が g_j より長いとすると $g_js_a{}^\epsilon$ は g_k のはじめの一部分となり, したがってGに属する. すなわち $\phi(g_js_a{}^\epsilon)=g_js_a{}^\epsilon$ が成り立つことになり, これから $v=1$ が得られて仮定に反する. したがって $v\neq 1$ は $gs^\epsilon\phi(gs^\epsilon)^{-1}$ なる形に一意的に表わされることになり, 特に v の主要因子はただ一つ存在することになる.

補題 7.2.4. $v_1\neq 1$, $v_2\neq 1$, $v_2\neq v_1{}^{-1}$ のとき v_1v_2 において簡約はどちらの v の主要因子にも到達しない.

証: $v_1=g_is_a{}^\epsilon g_j{}^{-1}$, $g_j=\phi(g_is_a{}^\epsilon)$, $v_2=g_ks_b{}^\eta g_l{}^{-1}$, $g_l=\phi(g_ks_b{}^\eta)$ とすると v_1, v_2 が既約に表わされていることと $v_2\neq v_1{}^{-1}$ から $g_k=g_j$, $s_b{}^{-\eta}=s_a{}^\epsilon$ のうち少なくとも一方は成立しない. いまこの補題が成り立たないとし簡約が主要因子にまでおよんだとしよう. まず $s_b{}^\eta$ だけが簡約されたとすると g_j のはじめの部分は $g_ks_b{}^\eta$ なる形をしているから $\phi(g_ks_b{}^\eta)=g_ks_b{}^\eta$ から $v_2=1$ が得られて仮定に反する. 同様にして $s_a{}^\epsilon$ だけが簡約されたとすると $g_js_a{}^{-\epsilon}$ が g_k のはじめの部分に現われることになり $v_1=1$ が得られて仮定に反する. またもし $s_a{}^\epsilon$, $s_b{}^\eta$ が同時に簡約されるとすれば $g_k=g_j$, $s_b{}^\eta=s_a{}^{-\epsilon}$ から $v_2=v_1{}^{-1}$ が得られ再び仮定に反する.

補題 7.2.5. $v_i\neq 1$ $(i=1,\cdots,m)$, $v_{i+1}\neq v_i{}^{-1}$ $(i=1,\cdots,m-1)$ のとき積 $v_1v_2\cdots v_m$ は1ではあり得ない.

証: 補題 7.2.4 を繰り返し使うと v_i と v_{i+1} の間の簡約はどちらの主要因子にも到達しないから既約形に表わしたとすると $v_1\cdots v_m$ はすべての主要因子を含むことになり1には等しくない.

さて $u=gs\phi(gs)^{-1}\neq 1$ なる元uを考える. 補題 7.2.2 からこのような元uの全体はUを生成する. このようなuのどんな積も既約語としてかいたとき1ではない, すなわち主要因子によって表わしたとき1まで簡約されない. そのようなuをUの**自由生成元** (free generator) ということにする. しかるにど

のような $v\neq1$ も u か u^{-1} のどちらか一方で表わされるから $u\neq1$ より生成される既約語は補題 7.2.5 であつかったような $v_i\neq1$, $v_{i+1}\neq v_i^{-1}$ に対して $v_1v_2\cdots v_m$ なる形をしているし，そのような語は1になることはない．したがって次の補題7.2.6が成立する．

補題 7.2.6. 元 $u=gs\phi(gs)^{-1}\neq1$ は U の自由生成元である．

このように U の自由生成元が見出されたので U は自由群である．

補題 7.2.4 における主要因子の役割が定理 7.2.1 の証明の鍵となる．この概念を主要因子からはなれた定義により一般化することができる．

元の集合 Y が $Y\cap Y^{-1}=0$ を満たし Y の各元 y に対し y と y^{-1} の既約形

$$y=a_1\cdots a_i\cdots a_t,$$
$$y^{-1}=a_t^{-1}\cdots a_i^{-1}\cdots a_1^{-1}$$

において任意の積

$$zw,\ z\neq w^{-1},\ \ z, w\in Y\cup Y^{-1}$$

の簡約が z, w の主要因子に到達しないように y から a_i, y^{-1} から a_i^{-1} を選ぶことができるとき Y は主要因子を持つという．換言すれば $Y\cup Y^{-1}$ の元の因子に対して補題7.2.4が成り立つとき Y は主要因子をもつ．集合 Y の元 y の主要因子は y の長さが奇数のときは中央に，y の長さが偶数のときは中央の二つのうちどちらか一方に主要因子があるとき**中心主要因子**（central significant factor）という．

定理 7.2.2. 集合 Y が主要因子をもてば Y はその元によって生成される部分群に対する自由生成元からなる．もし G が G の元 g が剰余類 Ug の中の最小の長さであるような Schreier 系とすると $u=gs\phi(gs)^{-1}\neq1$ を満たす u に対して現われる s 全体は中心主要因子の集合をなす．

証：主要因子の定義から $v_1, v_2\in Y\cup Y^{-1}$ に対して補題 7.2.4 は成立する．しからば補題 7.2.5 も成立する．したがって y の既約形が単位元でなければ y とその逆元から作られる語は単位元ではない．したがって y はそれらが生成する群の自由生成元である．

Gが，ある部分群Uによる剰余類Ugがgより短い長さをもつ元を含まないような代表系gからなる Schreier 系とすると

$$gs \in U\phi(gs),$$
$$\phi(gs)s^{-1} \in Ug$$

からgと $\phi(gs)$ がその長さにおいてたかだか1しか違わないことが分かる．このsは補題 7.2.4 により主要因子なることは分かっているが $u=gs\phi(gs)^{-1}$ においてたかだか1しか長さが違わない二つの語の間にあることから中心主要因子となる．

補題 7.2.6 と主定理の逆を証明しよう．

定理 7.2.3. 自由生成元の集合Sで生成される自由群Fのある Schreier 系をGとする．$g \in G$, $s \in S$ に対し $\phi(h)$ を元 $h=gs^\epsilon$, $\epsilon=\pm 1$, に対して定義され次の性質をもつ函数とする．

1） $\phi(gs^\epsilon) \in G$.

2） $gs^\epsilon \in G$ ならば $\phi(gs^\epsilon)=gs^\epsilon$.

3） $\phi[\phi(gs^\epsilon)s^{-\epsilon}]=g$.

このとき元 $u=gs\phi(gs)^{-1} \neq 1$ はFのある部分群Uの自由生成元であってこの Schreier 系はUのFの中での左剰余類の代表元の集合である．

証：一般的記号として $v=gs^\epsilon\phi(gs^\epsilon)^{-1}$ とかく．補題 7.2.3, 7.2.4, 7.2.5 の証明はここに与えられた仮定のもとで成立する．それは函数ϕの与えられた性質だけがそれらの補題の証明に使われたからである．補題7.2.5から元$u=gs\phi(gs)^{-1} \neq 1$ はFのある部分群Uの自由生成元である．

Schreier 系GがUによる左剰余類の代表元の集合であることを示すために $S \cup S^{-1}$ に含まれるすべての語fに対して函数 $\Phi(f)$ を定義しよう．

$$f=a_1a_2\cdots a_t, \quad a_i \in S \cup S^{-1}, \quad i=1, \cdots, t$$

のとき

$$h_0=1,$$
$$h_i=\phi(h_{i-1}a_i), \quad i=1, \cdots, t,$$

$$h_t=\Phi(f)$$

と置く.

$\Phi(f)$ の次の基本的な性質は容易に証明される.

1) $\Phi(a_1\cdots a_ia_{i+1}\cdots a_t)=\Phi(a_1\cdots a_is^{\epsilon}s^{-\epsilon}a_{i+1}\cdots a_t)$.

定義からどの h_i $(i=1,\cdots,t)$ も G の元であるから右辺を計算することにより性質(3)から順次 h_i, $\phi(h_is^{\epsilon})$, $\phi[\phi(h_is^{\epsilon})s^{-\epsilon}]=h_i$ が得られそれ以外は両辺の計算は同じである. したがって F のある元を代表とする任意の語 f を持ってきても $\Phi(f)$ の値は等しい.

2) $\Phi(g)=g$.

G の元 g の既約形を $g=a_1\cdots a_t$ とすれば g のどの初めの部分も G に含まれるから性質(2)によって $h_i=a_1\cdots a_i$ $(i=1,\cdots,t)$ となる.

3) $\Phi(f_1f_2)=\Phi[\Phi(f_1)f_2]$.

$f_1=a_1\cdots a_i$, $f_2=a_{i+1}\cdots a_t$, $f=f_1f_2$ とかくと $h_i=\Phi(f_1)$ は G の元であるから $\Phi(h_i)=h_i$ が成立する. したがって $\Phi(h_if_2)$ を計算すれば途中で h_i が得られ順次 $h_{i+1},\cdots,h_t=\Phi(f_1f_2)$ が得られる.

4) $\Phi(gs^{\epsilon})=\phi(gs^{\epsilon})$.

Φ の定義から $\Phi(gs^{\epsilon})=\phi(\Phi(g)s^{\epsilon})$ が成立する. したがって $\Phi(gs^{\epsilon})=\phi(gs^{\epsilon})$ が $\Phi(g)=g$ から得られる.

5) $\Phi[gs^{\epsilon}\phi(gs^{\epsilon})^{-1}]=1$.

$\Phi[gs^{\epsilon}\phi(gs^{\epsilon})^{-1}]=\Phi[\Phi(gs^{\epsilon})\phi(gs^{\epsilon})^{-1}]=\Phi[\phi(gs^{\epsilon})\phi(gs^{\epsilon})^{-1}]=\Phi(1)=1$ なることから明らかである.

6) $f\in U$ ならば $\Phi(f)=1$ である.

これは 3), 5) を繰り返し使えばよい.

7) $\Phi(f)=g$ ならば $f\in Ug$ である.

$$\begin{aligned} f&=a_1a_2\cdots a_t \\ &=(1\cdot a_1\cdot h_1^{-1})(h_1a_2h_2^{-1})\cdots(h_{t-1}a_th_t^{-1})h_t \end{aligned}$$

であって $h_t=\Phi(f)=g$ と $h_{i-1}a_ih_i^{-1}=gs^{\epsilon}\phi(gs^{\epsilon})^{-1}\in U$, $(i=1,\cdots,t)$ から得られる. とくに $\Phi(f)=1$ ならば $f\in U$ が成り立つ.

8)　$g_i \neq g_j$ ならば g_i と g_j はUの異なる剰余類に含まれる.

もしこれが成り立たないとするとUの元wが存在して $g_i = wg_j$ とかけ $g_i = \Phi(g_i) = \Phi[\Phi(w)g_j] = \Phi(g_j) = g_j$ となり矛盾が得られる.

したがって剰余類Ugはすべて異なりそれら全体でFとなる. 定理7.2.3の証明において必要とされたこと以上のことが分かったのでこれを定理としよう.

定理 7.2.4. Schreier 系Gと定理 7.2.3 での函数 $\phi(gs^{\epsilon})$ が与えられただけで任意の元fがGとϕによって定まるUに属しているか否かを判定することができる.

証: ϕ とGから $\Phi(f)$ を計算することができ $\Phi(f)=1$ と $f \in U$ とは同値である.

このようにϕとGはUを明確に定めるからϕとGがUを表わしているものとみなし, $U=U[G, \phi(gs^{\epsilon})]$ をUの**標準的表現** (standard representation) ということにする.

自然に次のような疑問が起こる.

1)　同じ部分群の異なる標準的表現は互いにどのような関係にあるか.

2)　与えられた Schreier 系からどれほどの部分群が表現されるか.

次にこの疑問に答えよう.

定理 7.2.5. $U_1 = U_1[G_1, \phi_1(gs^{\epsilon})]$, $U_2 = U_2[G_2, \phi_2(gs^{\epsilon})]$ が同じ部分群になるための必要十分条件は Schreier 系 G_1, G_2 の間に $1 \leftrightarrows 1$ なる一対一対応 $g^1 \leftrightarrows g^2$ があり $g^1 \leftrightarrows g^2$ ならば任意の s^{ϵ} に対し $\phi_1(g^1 s^{\epsilon}) \leftrightarrows \phi_2(g^2 s^{\epsilon})$ となることである.

証: もし $U_1 = U_2 = U$ ならばUのどの剰余類も G_1 および G_2 から代表元を選ぶことができる. もし $Ug^1 = Ug^2$ であれば対応 $g^1 \leftrightarrows g^2$ は明らかに一対一であり $1 \leftrightarrows 1$ が成り立つ. $g^1 s^{\epsilon}$ と $g^2 s^{\epsilon}$ は同じ剰余類に入るから $\phi_1(g^1 s^{\epsilon}) \leftrightarrows \phi_2(g^2 s^{\epsilon})$ が成り立つ.

逆に $1 \leftrightarrows 1$ なる一対一対応 $g^1 \leftrightarrows g^2$ が $\phi_1(g^1 s^{\epsilon}) \leftrightarrows \phi_2(g^2 s^{\epsilon})$ を満たしている

とすれば任意の f に対し $\Phi_1(f) \leftrightarrows \Phi_2(f)$ となる．とくに $\Phi_1(f)=1$ と $\Phi_2(f)=1$ とは同じ条件であるから U_1 と U_2 は同じ元からなりしたがって同一の部分群となる．さらに g^1 の長さに関する帰納法により $Ug^1=Ug^2$ もいえる．

第二の疑問に答える前に函数 ϕ のいくつかの性質を述べよう．生成元 s を固定したとき $g\in G$ に対し写像 $\pi(s): g\to\phi(gs)$, $\pi(s^{-1}): g\to\phi(gs^{-1})$ は G を G の中に写す．ϕ の性質（3）から $\pi(s)\pi(s^{-1})$ および $\pi(s^{-1})\pi(s)$ は恒等写像であるから $\pi(s)$ と $\pi(s^{-1})$ は置換（一対一写像）であって互いに逆置換である．さらに（2）から ϕ によるある値は部分群 U に対してではなく G の性質によってのみ定まる．再び固定された s とすべての G の元 g を考える．G の元 g は次のような二つの類 $C(s), C^*(s)$ に分けられる．

$$g\in C(s) \iff^{1)} gs\in G,$$

$$g\in C^*(s) \iff gs\notin G.$$

類 $C(s), C^*(s)$ の濃度をそれぞれ $N(s), M(s)$, また G の濃度を N とすると

$$N(s)+M(s)=N$$

が成り立つ．同様に

$$g\in C(s^{-1}) \iff gs^{-1}\in G,$$

$$g\in C^*(s^{-1}) \iff gs^{-1}\notin G$$

と定義し $C(s^{-1}), C^*(s^{-1})$ の濃度をそれぞれ $N(s^{-1}), M(s^{-1})$ と置くと

$$N(s^{-1})+M(s^{-1})=N$$

が成立する．

さて G の元 g_i, g_j に対し $g_is=g_j$ が成り立てば $g_js^{-1}=g_i$ であるから $g_i\in C(s)$, $g_j\in C(s^{-1})$ となる．この関係から $C(s)$ と $C(s^{-1})$ の間には一対一対応があるから

$$N(s)=N(s^{-1})$$

が成立する．もし N が有限ならば次の式も成り立つ．

$$M(s)=M(s^{-1}).$$

しかし N が無限のときは任意の Schreier 系に対して $M(s)=M(s^{-1})$ が成り

---

1) $A \iff B$ は命題 A と命題 B とが同値なることを表わすものとする．

立つとは限らない．たとえば Schreier 系を $\{1, s, s^2, \cdots\}$ とすれば $M(s)=0$, $M(s^{-1})=1$ である．これに反し与えられたGに対しϕが存在すれば $\pi(s)$ は $C(s)$ を $C(s^{-1})$ の上に写像し，置換であるから $C^*(s)$ を $C^*(s^{-1})$ の上に写す．したがってϕが存在するためには $M(s)=M(s^{-1})$ なることが必要となる．

定理 7.2.6. 任意の生成元 s に対し $M(s)=M(s^{-1})$ が成り立つような Schreier 系Gが与えられたとする．そのとき次の三つの条件を満たす函数 $\phi(gs^{\epsilon})$ を見出すことができる．

1） $\phi(gs^{\epsilon})$ はGの元である．

2） $gs^{\epsilon}\in G$ ならば $\phi(gs^{\epsilon})=gs^{\epsilon}$.

3） $\phi[\phi(gs^{\epsilon})s^{-\epsilon}]=g$.

最も一般的なϕの取り方は次のように各sに対し定めるものである．

i） gs がGの元のときは $\phi(gs)=gs$.

ii） gs がGの元とならないようなgに対しては $\phi(gs)$ は $\pi(s): g\rightarrow\phi(gs)$ がGの置換になるように定める．

iii） すべての元gに対し $\phi(gs)$ が定義されたとき $\phi(gs^{-1})$ は $\pi(s^{-1}): g\rightarrow \phi(gs^{-1})$ が $\pi(s)$ の逆置換となるように定める．

証：すべての生成元sに対して $M(s)=M(s^{-1})$ が成立する条件からただ $\phi(gs^{\epsilon})$ が存在するというだけではなくもし構成することができるならば最も一般的な構成法が何であるかということもこの定理は示している．さて $\phi(gs^{\epsilon})$ の構成法の正しいことを示そう．与えられたsに対して明らかに

1） $\phi(gs)$ はGの元である，

2） gs がGの元であれば $\phi(gs)=gs$,

が成立する．もしある元 g_i に対し $g_is=g_j\in G$ ならば $\phi(g_is)=g_j$ と定めたことと $g_js^{-1}=g_i$ から対応 $g\rightarrow\phi(gs)$ によって $C(s)$ は $C(s^{-1})$ の上に写される．残りの $M(s)$ 個の元は $M(s^{-1})$ 個の元に写されるが $M(s)=M(s^{-1})$ なることから $C^*(s)$ を $C^*(s^{-1})$ の上に写す一対一対応を作ることが可能である．この対応を $g\in C^*(s)$ に対し $g\leftrightarrows g'\in C^*(s^{-1})$ と表わし $g'=\phi(gs)$ と置

く．このとき $\pi(s): g \leftrightarrows \phi(gs)$ は $C(s)$ を $C(s^{-1})$ の上にまた $C^*(s)$ を $C^*(s^{-1})$ の上に写す一対一対応である．さて $\pi(s)$ は置換であるから $\pi(s)$ の逆写像として $\pi(s^{-1}): g \leftrightarrows \phi(gs^{-1})$ と定めると $\phi(gs^{-1})$ の値が定まり明らかに $\phi(gs^{-1})$ はGの元である．また $\pi(s)$ は $C(s)$ を $C(s^{-1})$ の上に写すから次のことが導かれる．

3） gs^{-1} がGの元であれば $\phi(gs^{-1})=gs^{-1}$.

このように性質（1）と（2）はすべてのGの元gと s, s^{-1} に対して成立する．最後に性質（3）であるが $\pi(s)$ と $\pi(s^{-1})$ が逆写像であるから $\phi[\phi(gs^{\epsilon})s^{-\epsilon}]=g$ となる．定理 7.2.5 と定理 7.2.6 において置換 $\pi(s)$ は中心的な役割をなした．

もし $g=a_1a_2\cdots a_t$ ならば置換 $\pi(a_1)\pi(a_2)\cdots\pi(a_t)$ は1をgに写すから置換 $\pi(s)$ はG上に可移的な群を生成する．次の定理から分かるようにこのような置換だけで部分群Uが一意的に定まる．

定理 7.2.7. Fを自由生成元の集合Sで生成された自由群とする．またSの各元 s に対し $\pi(s)$ を集合 $1, y_2, y_3, \cdots$ に作用する置換とし $\pi(s)$ で生成される置換群がその集合上可移的であるとする．F の各元 $f=a_1a_2\cdots a_t$ に対し置換 $\pi(f)=\pi(a_1)\pi(a_2)\cdots\pi(a_t)$ を対応させる．しからば $\pi(f)$ が元 1 を固定するような元fの全体はある部分群Uをなす．もし $g_1=1,\ g_2, \cdots, g_i, \cdots$ がUによる左剰余類を代表するものからなる Schreier 系とすれば $\pi(g_i)$ が1を y_i に写す対応 $g_i \leftrightarrows y_i$ が考えられる．このようにして y_i 上の置換 $\pi(s)$ 全体は定理 7.2.5 および定理 7.2.6 における g_i 上の置換 $\pi(s)$ 全体と置換同型となる．

証：$\pi(f)$ が1を固定するようなf全体はFの部分群Uをなすことは明らかである．定理 5.3.1 から置換 $\pi(f)$ は1をUにまた元yをU以外のUの左剰余類で置き換えることによるFのUの剰余類の上への表現とみなされる．したがって各 y_i に対し $\pi(g_i)$ が1を y_i に写すような左剰余類 Ug_i が一意的に対応する．この表現において $\pi(s)$ は剰余類 Ug を剰余類 Ugs に写す．したが

って剰余類 Ug_i をその代表元 g_i で置き換えるならば $\pi(s)$ は定理 7.2.5 および定理 7.2.6 における $\pi(s)$ と同じとみなせるから $\mathcal{Y}$ の上の置換全体と Schreier 系G上の置換全体とが置換同型となる.

有限生成な自由群の有限指数をもつ部分群Uに対してUの生成元の個数とそれらの長さの合計を正確に計算することができる.

定理 7.2.8. r 個の自由生成元 $s_1, s_2, \cdots, s_r$ を持つ自由群 F_r の有限指数の部分群を $U=U[G, \phi(gs^\epsilon)]$ とすると

1) Uは $1+n(r-1)$ 個の自由生成元を持つ自由群である.

2) Schreier 系Gの元の長さの合計を L とすれば U の自由生成元 $u=gs\phi(gs^{-1})\neq 1$ の長さの合計は $K=(2L+n)r-2L$ で与えられる.

証: Uの自由生成元は次の形の元のうち単位元でないものであることはすでに示した.

$$u_{ia}=g_is_a\phi(g_is_a)^{-1},\quad i=1,\ \cdots, n\ ;\ a=1, \cdots, r.$$

また補題 **7.2.3** から u_{ia} は既約に表わされているか単位元である. さて s_a を固定させたとき $\phi(g_is_a)$ はGの置換であるから

$$\sum_{i=1}^{n} L(g_i)+L(s_a)+L[\phi(g_is_a)]=2L+n$$

が成り立つ. したがって既約形に直す前には長さの合計が $r-(2L+n)$ なる nr 個の元uがあるからこの合計から u_{ia} が単位元になるものの個数とそのuの長さ $L(g_i)+L(s_a)+L(g_is_a)$ を引き去らねばならない. u_{ia} が単位元になるのはどんなときか? g_i, s_a と $\phi(g_is_a)^{-1}$ が既約に表わされているから補題 7.2.3 からそれらが簡約されるとすれば $u_{ia}=1$ でありそのようになるのは s_a が g_i で簡約されるかまたは $\phi(g_is_a)^{-1}$ で簡約されるときである. 前者の場合 g_i は s_a^{-1} で終り既約に表わされた $g_j\in G$ に対し $g_i=g_js_a^{-1}$ とかける. また後者の場合は $\phi(g_is_a)=g_k$ は s_a で終り $g_k=g_is_a$ と表わされている. このようにして s_a に対して単位元となるuの個数は s_a か s_a^{-1} で終っているようなgの個数に等しくなる. しかるに $g=1$ を除きすべてのgは s_a か s_a^{-1} で終っ

ているからちょうど一度ずつこの数えた中に現われる．したがって全部で $(n-1)$ 個の u が単位元となり $nr-(n-1)=n(r-1)+1$ 個の U の自由生成元である u が残ることになる．長さについてはどうだろうか？ まず $g_i=g_js_a^{-1}$ であれば $\phi(g_is_a)=g_j$ から $L(g_i)+L(s_a)+L[\phi(g_is_a)]=2L(g_i)=2L(g_js_a^{-1})$ が成り立つ．次に $g_is_a=g_k$ とすると $L(g_i)+L(s_a)+L[\phi(g_is_a)]=2L(g_is_a)$ となる．このように s_a に対し s_a か s_a^{-1} で終る g の長さは $u_{ia}=1$ に対しては二度数えていたことになる．したがってすべての s_a に対し $g=1$ 以外のすべての g の長さが単位元に等しい u に対し二度数えられたことになる．一方 $L(1)=0$ であるから丁度 $2L$ だけ減ずればよい．すなわち U の自由生成元の長さの合計は $(2L+n)r-2L$ である．

最後に定理 7.2.7 を使って F_r の中で指数 n の部分群の個数を帰納的に求めよう．

定理 7.2.9. F_r に含まれる指数 n の部分群の個数 $N_{n,r}$ は次のように帰納的に与えられる．

$$N_{1,r}=1$$

$$N_{n,r}=n(n!)^{r-1}-\sum_{i=1}^{n-1}(n-i)!^{r-1}N_{i,r}$$

証：$N_{1,r}=1$ は F_r の指数 1 の部分群が F_r 自身なることと同じである．$1, x_2, \cdots, x_n$ 上の r 個の置換 $P_1, P_2, \cdots, P_r$ を選ぶ．一般に $P_1, P_2, \cdots, P_r$ で生成された群が $1, x_2, \cdots, x_n$ 上で可移的である必要はない．1 を含む可移域を $1, b_2, \cdots, b_t$ とし残りの文字を無視し $\pi(s_1), \pi(s_2), \cdots, \pi(s_r)$ を $1, b_2, \cdots, b_t$ 上の置換と考えると定理 7.2.7 からこれらは指数 t の部分群を一意的に定める．$P_1, P_2, \cdots, P_r$ により残りの $(n-t)$ 個の文字は $[(n-t)!]^r$ 通りにうごきうる．さらに $1, b_2, \cdots, b_t$ を $1, c_2, \cdots, c_t$ で置き換え残りの $(n-t)$ 個を自由に動かしても同じ部分群を定めるから合計で

$$(n-1)(n-2)\cdots(n-t+1)[(n-t)!]^r=(n-1)![(n-t)!]^{r-1}$$

通りの異なる置換 $P_1, P_2, \cdots, P_r$ が指数 t の同じ部分群を定める．$P_1, P_2, \cdots, P_r$ の選び方はそれらが定める部分群の指数にしたがって $(n!)^r$ 通り考えら

れるから

$$\sum_{t=1}^{n}(n-1)![(n-t)!]^{r-1}N_{t,r}=(n!)^r$$

が成立する．両辺を $(n-1)!$ で割り 1 から $(n-1)$ までの和を移項することにより定理に与えられた公式をうる．

7.3. 自由群の部分群の自由生成元．Nielsen の方法

7.2 節では自由群 F の部分群 U の性質を F における U の剰余類の立場から調べた．この節ではより直接に U の元について調べよう．

添数 i の集合 I により添数づけられた自由群 F の元の集合を $A=\{a_i\}$ とする．また A の元で生成される群を $[A]$ とかくときは A の元はその群の自由生成元であるとする．元 $f\in[A]$ に対して A の元 a とその逆元により f を既約語として表わしたときの長さを $L_A(f)$ とかく．

X を自由群 F の自由生成元の集合とする．F の元の集合 A が X に関して **Nielsen の性質**を持つとは

1) $A\cap A^{-1}=0$ (A^{-1} は A の元の逆元の集合である),

2) $a, b\in A\cup A^{-1}$, $L_X(ab)<L_X(a)$ ならば $b=a^{-1}$,

3) $a, b, c\in A\cup A^{-1}$, $L_X(abc)\leq L_X(a)-L_X(b)+L_X(c)$ ならば $b=a^{-1}$ であるか $b=c^{-1}$,

が成立するときである．

定理 7.3.1. F の自由生成元からなる集合 X に関して A が Nielsen の性質を持てば A の元は A により生成される部分群 $[A]$ の自由生成元である．Nielsen の性質は A の元の中に中心主要因子が存在することと同値である．

証：Nielsen の性質が中心主要因子の存在と同値であることを示せば十分である．なぜならば定理 7.2.2 からこれは A が $[A]$ の自由生成元からなることを意味するからである．

A が Nielsen の性質を持つとする．性質 (2) から $b\neq a^{-1}$ のときは

$L_X(ab) \geqq L_X(a)$, $L_X(b^{-1}a^{-1}) \geqq L_X(a^{-1})$ が得られ，したがって $L_X(ab) \geqq L_X(b)$ が成立する．ab から既約形を作るとき一方の因子たとえばそれを b とすると b の因子の 1/2 より多くが a の因子で簡約されたとすると $a=uv^{-1}$, $b=vw$ と置いて $L_X(v)>L_X(w)$, $L_X(ab)=L_X(uw)<L_X(u)+L_X(v)=L_X(a)$ が得られることになり矛盾である．したがってこのようなことは起こり得ないからたかだか a か b の因子の半分が ab の既約形を作るときに簡約されるだけである．したがって奇数の長さをもつ元に対してはその中央元が主要因子となる．またもし b が偶数の長さを持つときは b の最初の半分 v が $b \neq a^{-1}$ であれば ab の積をつくるとき簡約されることが考えられる．もし $b \neq c^{-1}$ であって b の後半分 w が bc の既約形を作るとき簡約されるとすれば $a=uv^{-1}$, $b=vw$, $c=w^{-1}z$ と置くと $L_X(abc)=L_X(uz) \leqq L_X(u)+L_X(z)=L_X(a)-L_X(b)+L_X(c)$ が得られ Nielsen の性質（3）に反する．したがってこのようなことは起こりえないから b の半分 u か w はどのように積をつくっても簡約されてしまうことはないからこの半分に属する b の二つの中央元のうち一方が中心主要因子となる．したがって Nielsen の性質から中心主要因子の存在が示される．逆に $A \cap A^{-1}=0$ を満たす集合 A に対し中心主要因子が存在するとする．もし $b \neq a^{-1}$ ならばたかだか b の半分が ab の既約形において簡約されそれと同数の因子が a で簡約されるから $L_X(ab) \geqq L_X(a)+L_X(b)-2 \cdot 1/2\, L_X(b)=L_X(a)$ が成り立ちしたがって 2) が成立する．また $b \neq a^{-1}$, $b \neq c^{-1}$ のとき積 abc から既約形をつくるとき a と b および b と c の間での簡約は b の主要因子まで到達しないから $L_X(abc)>L_X(a)+L_X(b)+L_X(c)-2L_X(b)$ が成立し 3) が示される．3) と主要因子の存在とが同値なることを示すのは難しくはない．なぜならば与えられた b に対し $a \neq b^{-1}$ なる元 a で b の左側の因子を最大限に簡約するようにとりまた $c \neq b^{-1}$ なる元 c として b の右側の因子を最大限に簡約するようにとる．3) は b の因子のすべては簡約されないことを意味しているから簡約されない任意の b の因子が主要因子になりうる．

定理 7.3.2. 自由生成元の集合Xにより生成される自由群の有限個の元 $\beta_1, \beta_2, \cdots, \beta_m$ からなる集合をBとする. 次の型の有限回の置換で集合Bを, Aで生成される群とBで生成される群が等しくかつAはXに関して Nielsen の性質を持つような集合 A ; $\alpha_1, \cdots, \alpha_n$, $n \leqq m$, で置き換えることができる.

1型 $\beta_i = 1$ を除く.

2型 β_i を β_i^{-1} で置き換える.

3型 β_j を $\beta_i\beta_j$ $(i \neq j)$ で置き換える.

したがってAは $[A]=[B]$ の自由生成元の集合である.

証: この各置換は集合を, 同じ群を生成する他の集合に写すことは明らかである. 1型は元の数を減らし, 2, 3型は元の数は変えない. 2, 3型の置換の合成により β_j を $\beta_i^{\epsilon}\beta_j^{\eta}$ か $\beta_j^{\eta}\beta_i^{\epsilon}$, $\epsilon=\pm 1$, $\eta=\pm 1$, に置換他のβを不変にする.

もし二つのβが等しいか逆元であれば一方のβを1で置き換え, しかる後この1を取り去ることができる. これはβの数を減らすからたかだかm回しか起こりえない. もし $a, b \in B \cup B^{-1}$, $b \neq a^{-1}$ のとき $L_X(ab) < L_X(a)$ とすると $L_X(a^2) > L_X(a)$ であるから $b=a$ は成立しない. したがって $\beta = a^{\epsilon}$ を ab で置き換えることができ各βの長さの合計を減らすことができるからこのような置き換えは有限回しか起こり得ず, 有限回の置き換えにより Nielsen の性質 (1), (2) を満たすようにできる. 性質 (3) を満足させることはより複雑である.

集合Xが無限であるか否かを問わず各βの中に現われるXに含まれた生成元の集合Yは有限である. Yで生成されるFの元を長さの順にならべる. ただし同じ長さのものは任意の順序でならべるが一度ならべるとその順序は固定させる. 同じ長さの元の数は有限であるからこの表においては各元の前には有限個の元しか存在しない.

βの長さが偶数 $2k$ のとき γ, δ を長さkの元として $\beta=\gamma\delta^{-1}$ とかく. $\beta \neq 1$ であれば $\gamma \neq \delta$ である. $\beta^{-1}=\delta\gamma^{-1}$ であるから必要ならばβを β^{-1} で置き換え

ることによりその前半分が後半分よりこの表で前にあるとしてよい．もし $\beta_i=\gamma\delta^{-1}$ であってある β_j が δ ではじまっているときは $\beta_j=\delta z$ を $\beta_i\beta_j=\gamma z$ で置き換える．同様にもし β_k が δ^{-1} で終っているならば $\beta_k=w\delta^{-1}$ を $\beta_k\beta_i^{-1}=w\gamma^{-1}$ で置き換える．このように $\beta_i=\gamma\delta^{-1}$ であれば β を置き換えることにより β_i 以外の β は δ ではじまることも δ^{-1} で終わることもないようにできる．δ をこの表で前にある同じ長さの γ で置き換えていくことからこの操作は有限回で終わる．もし偶数の長さを持つ最短の元 β からはじめ，より長い偶数の長さを持つ元 β に対してこの操作を続けていけば，すべては有限回で終わることに注意しよう．$\beta_i=\gamma\delta^{-1}$ より長い β に対しては δ ではじまることも δ^{-1} で終わることもない．もちろんそれらの過程で条件 $A\cap A^{-1}=0$ か $L_X(ab)\geqq L_X(a)$ が成立しなくなるときは適当な置き換えをほどこし β の数を減らすかまたは長さの合計を減して後，β の数や長さをかえないこの置き換えを行なえばよい．置き換えを有限回行なうことによりこの操作が終わり $\alpha_1, \cdots, \alpha_n$, $n\leqq m$, からなる集合 A が得られる．この集合 A が X に関して Nielsen の性質を満たすことを示そう．$A\cap A^{-1}=0$, および $a, b\in A\cup A^{-1}$, $b\neq a^{-1}$ のとき $L_X(ab)\geqq L_X(a)$ は確かに成立している．なぜならばもし成立していないとすると β の数か長さの合計を減らすことができるからである．$b\neq a^{-1}$, $b\neq c^{-1}$ のとき積 abc を考える．もし b の長さが奇数 $2k+1$ であれば b のはじめのたかだか k 個の因子が a により簡約されまた終わりのたかだか k 個の因子が c により簡約されるだけであるから $L_X(abc)>L_X(a)-L_X(b)+L_X(c)$ が成り立つ．もし b が偶数の長さを持つとすれば b は δ より(この表で)前にある γ に対して $\gamma\delta^{-1}$ か $\delta\gamma^{-1}$ なる形をしているから第二の性質によって（すでにその性質の成立は上に示した）たかだか b の半分の因子しかそれぞれ a, c で簡約されない．しかるに a は δ^{-1} で終わっていないか c が δ ではじまっていないかが成立しているから b の半分すなわち δ または δ^{-1} すべてが簡約されることはない．したがって b がすべて簡約されてしまうことはないから $L_X(abc)>L_X(a)-L_X(b)+L_X(c)$ が成立し Nielsen の第三の性質が A に対して成立することになる．

定理 7.3.3. 二つの自由群が同型であるための必要十分条件はそれらの自由生成元の濃度が等しいことである．有限な r 個の自由生成元で生成される自由群 F_r はもし他の r 個の元で生成されているならばそれらで自由に生成されている．

証：F_X, F_Y をそれぞれ自由生成元の集合 X, Y 上の自由群とする．もし X, Y の濃度が等しいとすると X と Y の間に一対一対応が存在しその対応は F_X, F_Y の間の一対一対応に拡張できそれは明らかに同型対応である．

逆に F_X と F_Y が同型であるとすれば F_X と F_Y は指数 2 の部分群を同じ濃度で含んでいる．指数 2 の部分群は位数 2 の群の上へのある準同型写像の核である．その準同型は単位元に写される生成元の集合を定めることにより完全に定まる．したがって生成元の集合 Z 上の自由群 F_Z の指数 2 の部分群の個数は Z の空でない部分集合の個数に等しくなる．この個数は Z が無限集合のときは可附番以上であり Z が有限な r 個の元からなる集合であれば 2^r-1 となる．したがって F_X と F_Y が同型であれば X と Y は同時に無限であるかまたは有限であり，後者のときは X と Y は同数の元からなる．また X, Y が無限のときは F_X と F_Y はそれぞれ X と Y と同じ濃度でありかつ F_X と F_Y は同じ濃度を持つから X と Y も同じ濃度となる．

さて F_r が $X: x_1, x_2, \cdots, x_r$, 上の自由群でありまた $\beta_1, \beta_2, \cdots, \beta_r$ により生成されているとする．定理 7.3.2 から何回か 1, 2, 3 型の置換を行なうことにより（$\beta_1, \cdots, \beta_r$ から）自由生成元 $\alpha_1, \cdots, \alpha_s$, $s \leq r$, が得られる．しからば $s=r$ でなければならないから 1 型の置換は使われていない．もし 2, 3 型の置換により集合 B から集合 B' が得られたとすると B, B' のいずれか一方が自由生成元からなるときは他方も自由生成元からなることが直ちに分かる．したがって $\alpha_1, \cdots, \alpha_r$ が F_r の自由生成元なることから $\beta_1, \cdots, \beta_r$ も F_r の自由生成元となる．

これでこの定理は証明されたが $\alpha_1, \cdots, \alpha_r$ について，より以上の結果をうることができる．α_i $(i=1, \cdots, r)$ は Nielsen の性質を持っているから中心主

要因子を持つ（定理 7.3.1)．またγをあるαかその逆元とし $\gamma_i\gamma_{i+1}\neq 1$ とすると元 x_i ($i=1, \cdots, r$) は $x_i=\gamma_1\cdots\gamma_m$ と表わせる．さてγの積の既約形は各々の中心主要因子を含むからγの積 $\gamma_1\cdots\gamma_m$ は一つの積となりそれが x_i に等しくなる．したがって x_i は α_j か α_j^{-1} である．したがってさらに2型の置換を行なえばαの集合は $x_1, \cdots, x_r$ をある順序にならべたものとなる．したがって順序を無視すれば任意の F_r の自由生成元 $\beta_1, \cdots, \beta_r$ もどのようにして $x_1, \cdots, x_r$ から得られるかがわかる．これから F_r の自己同型がどのようなものかを知ることができる．

定理 7.3.4. 有限なr個の生成元の集合X上の自由群 F_r のすべての自己同型は次の自己同型で生成される．

1） $P_{ij}: x_i\to x_j, x_j\to x_i,\ x_k\to x_k,\ k\neq i, j,$

2） $V_i: x_i\to x_i^{-1},\ x_j\to x_j,\ j\neq i,$

3） $W_{ij}: x_j\to x_ix_j,\ i\neq j,\ x_k\to x_k,\ k\neq j,$

ここで $i\neq j$ は $1, \cdots, r$ のどれかである．

証：これら P_{ij}, V_i, W_{ij} は確かに F_r の自己同型である．なぜならばこれらはXを，F_r を生成するr個の元の集合に写すからである．次に任意の自己同型がこれらの積で表わされることを示さなければならない．この定理の前に F_r の最も一般的な自己同型が $X: x_1, \cdots, x_r$, を生成元の集合 $B: \beta_1, \cdots, \beta_r$ で置き換えることによりえられることを示した．この集合BはXに次のような有限回の置換を順次行なうことにより得られる．

$$B=B_1, B_2, \cdots, B_{N-1},\quad B_N=X$$

$i=1, \cdots, N-2$ に対して B_i は B_{i+1} に定理 7.3.2 の2型か3型の置換をほどこして得られ，B_{N-1} は $B_N=X$ の置換により得られる，すなわち互換 P_{ij} の積により得られる（§ 5.4)．したがって $i=1, \cdots, N-2$ に対して B_{i+1} を B_i に置き換えることは B_{i+1} の元の自己同型 V_i または W_{ij} である．これらがXの元の自己同型 V_i, W_{ij} の言葉でいい表わされることを示さなければならない．

さて次のような F_r の自由生成元の三つの集合を考える.

$$Y: y_1, \cdots, y_r,$$
$$Z: z_1, \cdots, z_r,$$
$$W: w_1, \cdots, w_r,$$

ただし

1) $z_i = y_i^{-1}$, $z_j = y_j$, $j \neq i$

であるか

2) $z_j = z_i z_j$, $z_k = y_k$, $k \neq j$,

および

3) $w_m = z_m^{-1}$, $w_n = z_n$, $n \neq m$

であるか

4) $w_n = z_m z_n$, $w_t = z_t$, $t \neq n$,

とする.

Y を Z で置き換えることは Y に V または W なる自己同型をほどこすことであり, Z を W に置き換えることは Z に自己同型 V か W を作用させることである. (3) または (4) が Y 上の自己同型 V か W により得られることを示そう. いくつかの場合に分かれるがどの場合も比較的容易に示される. ここではそれらのうち最も面倒な二つの場合について示そう. まず $m=j$ であって (2) $z_j = y_i y_j$, (3) $w_m = z_m^{-1}$ とする. 自己同型 (3) が $y_i y_j$ を $y_j^{-1} y_i^{-1}$ に写し $k \neq j$ のとき y_k をうごかさないことを示さなければならない. これは y_j を $y_i^{-1} y_j^{-1} y_i^{-1}$ に写し他の y をうごかさないことと同値である. しかるにこれは $y_i \to y_i^{-1} y_j \to y_i^{-1} y_j^{-1} \to y_i^{-1} y_j^{-1} y_i^{-1}$ なる合成に等しくその合成は $W_{ij}^{-1}(y) V_j(y) W_{ij}(y)$ に等しい. 次に $m=j$, $n=i$ であって (2) $z_j = y_i y_j$, (4) $w_n = z_m z_n$ とする. 自己同型 (4) は $z_j = y_i y_j$ を $y_i y_j$ に, $z_i = y_i$ を $y_i y_j y_i$ に写し他のすべての $z_k = y_k$ はうごかさない. これは

$$y_i \to y_i y_j y_i,$$
$$y_j \to y_i^{-1}$$

なる置き換えと同じである. しかるにこれは次のように合成 $W_{ij}^{-1}(y) W_{ji}(y)$

$W_{ij}(y)$ に等しい.

$$y_i \to y_i \to y_j y_i \to v_i v_j y_i,$$
$$y_j \to y_i^{-1} y_j \to y_i^{-1} \to y_i^{-1}.$$

したがって Z 上の自己同型 V または W は Y 上の自己同型 V または W でいい表わすことができる. さて N に関する帰納法により定理の証明を続けることにしよう. 帰納法により B_{N-2} を B_1 で置き換えることは B_{N-2} の生成元の上での V か W の合成と仮定することができる. しかるに B_{N-1} を集合 Y と, また B_{N-2} を集合 Z とみなすと B_{N-2} を B_1 で置き換えることは集合 B_{N-1} 上での V か W で表わされ, B_{N-1} を B_{N-2} で置き換えることは B_{N-1} 上での V か W の作用に等しい. したがって B_{N-1} を B_1 で置き換えることは B_{N-1} 上で V か W を合成することに等しい. B_{N-1} が単に X 上の置換であるからこれは X 上での V か W の合成である. ゆえに定理は証明された.

A が F_X の自由生成元の集合 X に関して Nielsen の性質を持っているとき A は種々の方法で $[A]$ の"最短な"生成元の集合とみなすことができる.

定理 7.3.5. A が X に関し Nielsen の性質を持ち

$$f = a_1 a_2 \cdots a_t, \quad a_i \in A \cup A^{-1}, \quad a_i a_{i+1} \neq 1$$

が成り立てば

$$L_X(f) \geqq \tfrac{1}{2} L_X(a_1) + t - 2 + \tfrac{1}{2} L_X(a_t),$$
$$L_X(f) \geqq L_X(a_i \cdots a_j), \quad 1 \leqq i \leqq j \leqq t$$

が成立する. さらに X が有限であって A の元が長さの順に小さい方からならべられ

$$\alpha_1, \alpha_2, \cdots, \alpha_r, \cdots$$

でありまた

$$\beta_1, \beta_2, \cdots, \beta_i, \cdots$$

が長さの順に小さい方からならべられた A に対する他の自由生成元の集合とすれば

$$L_X(\beta_n) \geqq L_X(\alpha_n), \quad n = 1, 2, \cdots$$

が成立する.

証：$f=a_1a_2\cdots a_t$ において各 a_i は f の既約形をつくるとき簡約されない中心因子を持っているから f の既約形においては少なくとも a_1 の前半分, $a_2, \cdots, a_{t-1}$ の中心因子および a_t の後半分は残る. したがって $L_X(f)\geqq 1/2L_X(a_1)+t-2+1/2L_X(a_t)$ が成り立つ. $a_1a_2\cdots a_t$ の既約形において $a_1\cdots a_{t-1}$ と a_t の簡約は a_{t-1} と a_t のどちらの中心因子にも達しないから a_{t-1} の k 個の因子と a_t の k 個の因子が簡約されたとすると $k\leqq 1/2L_X(a_{t-1})$, $k\leqq 1/2L_X(a_t)$ が成り立つ. したがって $L_X(f)=L_X(a_1\cdots a_{t-1})+L_X(a_t)-2k$ が成り立つ. しかるに $2k\leqq L_X(a_t)$ であるから $L_X(a_1\cdots a_t)\geqq L_X(a_1\cdots a_{t-1})$ が成立する. 同様にして $L_X(a_1\cdots a_t)\geqq L_X(a_2\cdots a_t)$ も成立する. この論法を繰り返していくと $L_X(a_1\cdots a_t)\geqq L_X(a_i\cdots a_j)$ が得られる.

もし X が有限であれば与えられた長さの元は有限個しか存在しないから A の元を長さの順に小さい方からならべていくと A のすべての元がつくされる. これを $\alpha_1, \alpha_2, \cdots, \alpha_i, \cdots$ とする. 他の生成元に対しては $\beta_1, \beta_2, \cdots, \beta_i, \cdots$ とする. β のはじめの n 個を A の自由生成元で表わしたとき $\beta_1(\alpha), \cdots, \beta_n(\alpha)$ であるとし α_r をこの表現の中に現われる α の最後の元とすると $r\geqq n$ が成り立つ. もしこれが成立しないとし $r<n$ と仮定すると $[A]$ の交換子群 K を法として

$$\begin{gathered}\beta_1\equiv\alpha_1^{e_{11}}\cdots\alpha_r^{e_{1r}} \pmod{K},\\ \cdots\cdots\cdots\cdots\cdots\cdots,\\ \beta_n\equiv\alpha_1^{e_{n1}}\cdots\alpha_r^{e_{nr}} \pmod{K}\end{gathered}$$

が成り立つ. $r<n$ であるからすべては零ではない有理整数 $u_1, \cdots, u_n$ が存在して*)

$$\begin{gathered}e_{11}u_1+\cdots+e_{n1}u_n=0,\\ \cdots\cdots\cdots\cdots\cdots,\\ e_{1r}u_1+\cdots+e_{nr}u_n=0\end{gathered}$$

を満たす.

しからばすべては零ではない $u_1, \cdots, u_n$ に対して $\beta_1^{u_1}\cdots\beta_n^{u_n}\in K$ となり各 β

*) Birkhoff and MacLane [1], p. 48. 交換子群の性質については § 9.2 を参照.

が $[A]$ の自由生成元なることに反する．したがって $r\geqq n$ が成立する．α_r が $j\leqq n$ なる j に対し $\beta_j(\alpha)$ の中に現われたとすると定理の前半から $L_X(\beta_j)\geqq L_X(\alpha_r)$ が成り立つ．しかるに $r\geqq n$ であるから $L_X(\beta_n)\geqq L_X(\beta_j)$, $L_X(\alpha_r)\geqq L_X(\alpha_n)$ がしたがって $L_X(\beta_n)\geqq L_X(\alpha_n)$ が得られる．

演 習 問 題

1. Fを x, y で生成される自由群とする．このとき x^2yxy^{-1} を含むFの全不変部分群はF自身かFにおいて指数9の部分群なることを示せ．
2. 二つの生成元をもつ自由群の指数3の部分群をすべて求めよ．
3. Fを三元 a, b, c で生成された自由群とする．F の元の平方で生成される指数8の部分群の自由生成元の集合を求めよ．
4. $A_1, A_2, \cdots, A_m$ を自由群の既約に表わされた元としどの A_i も1ではなくかつ $A_1A_2\cdots A_m=1$ が成立しているとする．このとき積 $A_{i-1}A_iA_{i+1}$ において A_i が完全に簡約されてしまうような i が存在することを示せ．
5. 自由群Fにおいて既約語 $g=a_1a_2\cdots a_t\neq 1$ が与えられたとするとFには $g\notin H$ を満たす指数 $t+1$ の部分群Hが存在することを示せ．（ヒント：Hの剰余類の代表系として $1, a_1, a_1a_2, \cdots, a_1a_2\cdots a_t$ をとれ．）
6. 自由生成元 $x_1, \cdots, x_r$ で生成された自由群において $g=g(x_1, \cdots, x_r)$ を1と異なる語とすると元 $x_1, \cdots, x_r$ で生成された有限群GでGにおいてgが単位元とはならないものが存在することを示せ．（この章の問題5と第5章の問題1を使え．）

第8章　束と組成列

8.1.　部分順序集合

定　義：元の集合Sが部分順序集合であるとはSのある元の対(つい)に対して$a\supseteq b$（“aはbを含む” と読む）なる関係が定義されていて次の条件を満たすときである．

P1.　$a\supseteq a$.

P2.　$a\supseteq b$，$b\supseteq c$ ならば $a\supseteq c$ である．

P3.　$a\supseteq b$，$b\supseteq a$ ならば $a=b$ である．

定　義：部分順序集合Sの部分集合Tのすべての元tに対して $x\supseteq t$ であってxがSに含まれるときxをTの上界という．同様にTの各元tに対し $t\supseteq y$ となるSの元yをTの下界という．

定　義：xが次の条件を満たすときSの部分集合Tの最小上界という．

1)　xはTの上界である．

2)　zをTの任意の上界とすれば $z\supseteq x$ が成り立つ．

同様にyが次の条件を満たすときTの最大下界という．

a）yはTの下界である．

b）zをTの任意の下界とすれば $y\supseteq z$ が成り立つ．

一般に部分集合Tは最小上界または最大下界を持つとは限らない．しかしもしTが最小上界を持つとすれば定義から二つ以上の最小上界は互いに他を含むことになってP3から等しくなり，したがって最小上界は一意的に定まる．同じことが最大下界についてもいえる．

部分順序集合Sが次の条件を満たすとき**全順序集合**または**鎖**という．

P4. Sの任意の二元 a, b に対して $a \supseteq b$ か $b \supseteq a$ が必ず成り立つ.

$a \supseteq b$ のことを $b \subseteq a$ とかくこともある. また $a \supseteq b$ であって $a \neq b$ のとき $a \supset b$ とかく. 同様に $a \supset b$ を $b \subset a$ ともかく. また $a \supset b$ であり $a \supseteq x \supseteq b$ ならば $x = a$ か $x = b$ なるとき $a > b$ (“a は b の直後の元である” と読む) とかくことにする. $b < a$ は $a > b$ を意味するものとする.

例: Sを a, b, c, d, e, f からなる集合で次図においてxがyの上にあってxがyと結ばれているかまたは $x = y$ のとき $x \supseteq y$ と定義するとSは部分順序集合であって c, d からなる部分集合は上界は持たないが二つの下界 a, b を持つ. しかし最大下界は持たない.

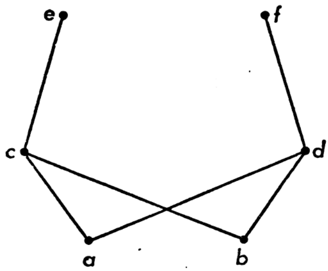


図 3. 部分順序集合

8.2. 束

定　義: 部分順序集合であってそれに含まれるどんな二元 a, b に対しても最小上界があり (これを和 $a \cup b$ とかく) また最大下界もある (積 $a \cap b$ とかく) とき束という.

$a \cup b$, $a \cap b$ はともに一意的に定まるから和と積は束における二元の間に定義された結合である.

定理 8.2.1. 束においては次の法則が成り立つ.

$L1$. 巾等律　$x \cap x = x$, $x \cup x = x$.

$L2$. 交換律　$x \cap y = y \cap x$, $x \cup y = y \cup x$.

$L3$. 結合律　$x \cap (y \cap z) = (x \cap y) \cap z$, $x \cup (y \cup z) = (x \cup y) \cup z$.

$L4$. 吸収律　$x \cap (x \cup y) = x$, $x \cup (x \cap y) = x$.

証: $L1, L2, L4$ は最小上界, 最大下界の定義から直接得られる. $L3$ を示すために $y \cap z = u$, $x \cap u = w$ と置く. このときwは x, u の下界であるから x, y, z の下界でもある. しかるに x, y, z のどんな下界もuに含まれるから $x \cap u$

$=w$ に含まれる．したがって w は x, y, z の最大下界である．同様にして $(x\cap y)\cap z$ が x, y, z の最大下界なることが示されるから $x\cap(y\cap z)=(x\cap y)\cap z$ が成り立つ．同様にして $x\cup(y\cup z)$, $(x\cup y)\cup z$ がともに x, y, z の最小上界なることが示される．

定理 8.2.2. $L1, L2, L3, L4$ で束は特徴づけられる．

証：$L1, L2, L3, L4$ を満たす任意の系においては $x\cap y=y$ と $x\cup y=x$ は同値である．そのような系において $x\cap y=y$ のとき $x\supseteq y$ と定義すればこの系は関係 $\supseteq$ に関して部分順序集合となる．$a\cap a=a$ から $P1$ が得られる．もし $a\cap b=b$, $b\cap c=c$ とすれば $a\cap c=a\cap(b\cap c)=(a\cap b)\cap c=b\cap c=c$ が成り立つから $P2$ が成立する．またもし $a\cap b=b$, $b\cap a=a$ であるとすれば $a\cap b=b\cap a$ であるから $P3$ が成り立つ．したがってこの包含関係によりこの系は部分順序集合となる．さらに $a\cap(a\cap b)=(a\cap a)\cap b=a\cap b$, $b\cap(a\cap b)=a\cap b$ から $a\cap b$ は a, b の下界である．一方 $a\supseteq x$, $b\supseteq x$ とすると $a\cap x=x$, $b\cap x=x$ であるから $(a\cap b)\cap x=a\cap(b\cap x)=a\cap x=x$ が成り立つ．したがって $a\cap b$ は a, b の最大下界となる．同様にして $y\supseteq a$, $y\supseteq b$ とすると $a\cup y=y$, $b\cup y=y$ が成り立ち，したがって $y=(a\cup b)\cup y$ が成立することになり $a\cup b$ が a, b の上界のみならず最小上界なることが分かる．

$L1, L2, L3, L4$ 以外の性質を持った束があるがその中で次の性質を持つものは重要である．

定　義：束 L_1 の元 x_i と束 L_2 の元 y_i の間に $x_i\cap x_j \leftrightarrows y_i\cap y_j$, $x_i\cup x_j \leftrightarrows y_i\cup y_j$ となるような一対一対応 $x_i \leftrightarrows y_i$ があるとき L_1 は L_2 に同型であるという．

定　義：束 L のどんな部分集合も最大下界，最小上界を持つとき L は完備であるという．また L のすべての元の集合が最小上界を持つときその元を全元といい，最大下界を持つときその元を零元という．

定　義：束 L が次の条件

$D_1.$ $$a\cap(b\cup c)=(a\cap b)\cup(a\cap c)$$

を満たすとき分配束であるという.

定　義：束Lが modular 束であるとは

(M) $$a\supseteq b \text{ ならば } a\cap(b\cup c)=b\cup(a\cap c)$$

が成立するときである.

束またはより一般に部分順序集合においてどのような鎖 $a_1\supset a_2\supset a_3\supset\cdots$ も有限鎖であるとき，その集合は**極小条件**を満たすといいまたどんな鎖 $a_1\subset a_2\subset a_3\subset\cdots$ も有限鎖のときその集合は**極大条件**を満たすという.

定　義：束Lにおいて有限鎖 $x=x_0\supseteq x_1\supseteq\cdots\supseteq x_d=y$ は $j=0,1,\cdots,d-1$ に対して x_i が x_{i+1} の直後の元のときすなわち $x=x_0>x_1>\cdots>x_d=y$ のとき極大であるといい，この鎖の長さはdであるという.

定　義：束Lが零元0を持ちLの元xと0を結ぶ任意の鎖が有限鎖であってxと0を結ぶ最長極大鎖の長さがdのとき元xは有限次元dを持つといいその次元を $d(x)$ とかく.

8.3. Modular 束と半 Modular 束

任意の束において $a\supseteq x\supseteq b$ を満たす元xの全体は部分束をなすがこれを**商** a/b という．二つの商 $a\cup b/b$, $a/a\cap b$ は互いに**転置される** (perspective) といい，また $i=1,\cdots,n-1$ に対して a_i/b_i が a_{i+1}/b_{i+1} に転置されるとき a_1/b_1 は a_n/b_nに**射影される** (projective) という.

定理 8.3.1. modular 束においては互いに転置される商は同型である.

証：modular 束において商 $a\cup b/b$, $a/a\cap b$ が与えられたとする．$a/a\cap b$ の任意の元xに対し

$$y(x)=x\cup b$$

と定義する．また $a\cup b/b$ の任意の元yに対し

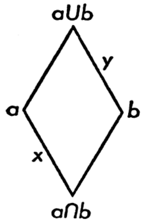


図 4. 転置商

$$x(y)=y\cap a$$

と置くと最初の定義から $a/a\cap b$ から $a\cup b/b$ の中への写像が，また第二の定義から $a\cup b/b$ から $a/a\cap b$ の中への写像がそれぞれ定義される．$a/a\cap b$ の元 x に対し $x[y(x)]=(x\cup b)\cap a$ が成り立ち $a\supseteq x$, $x\supseteq a\cap b$ から modular 律を使うと $a\cap(x\cup b)=x\cup(a\cap b)=x$ が，したがって $x[y(x)]=x$ が成立する．同様にして $a\cup b/b$ の元 y に対し modular 律を使って $y[x(y)]=y$ をうる．したがって $x\to y(x)$, $y\to x(y)$ は二つの商の間の一対一対応を与える．さらにこの対応は束の演算を保存する．$a/a\cap b$ の元 x_1, x_2 に対し $y(x_1\cup x_2)=(x_1\cup x_2)\cup b=(x_1\cup b)\cup(x_2\cup b)=y(x_1)\cup y(x_2)$ が成り立ちまた $x_1=x(y_1)$, $x_2=x(y_2)$ とすると $x_1\cap x_2=x(y_1)\cap x(y_2)=(y_1\cap a)\cap(y_2\cap a)=y_1\cap y_2\cap a=x(y_1\cap y_2)$ が成り立つ．したがって $y(x_1\cap x_2)=y[x(y_1\cap y_2)]=y_1\cap y_2=y(x_1)\cap y(x_2)$ が成立し写像 $x\to y(x)$ は両演算を保存する．この対応は一対一であるから $x\to y(x)$ によりすべての演算が保存されることになる．同様にして $y\to x(y)$ が両演算を保存することを証明することができる．

系 8.3.1. modular 束においては射影商は同型である．

定理 8.3.2. modular 束において元 x が有限次元 $d(x)$ を持つとき x と 0 を結ぶ任意の極大鎖は同じ長さを持つ．

証：x の次元に関する帰納法で証明する．もし $d(x)=1$ とすれば $x>0$ が x と 0 を結ぶただ一の鎖である．$x=x_0>x_1>\cdots>x_d=0$, $x=y_0>y_1>\cdots>y_s=0$ を x と 0 とを結ぶ二つの極大鎖としよう．もし $x_1=y_1$ であれば帰納法の仮定から x_1, y_1 からの極大鎖は同じ長さ $d-1$ を持つことになり $s-1=d-1$ が，したがって $s=d$ が成り立つ．もし $x_1\neq y_1$ とすると $z_2=x_1\cap y_1$ と置くと x/x_1, y_1/z_2 および x/y_1, x_1/z_2 はそれぞれ転置される．x/x_1, x/y_1 はともに中間の元を含まないから $y_1>z_2$, $x_1>z_2$ となる．仮定から x_1 と 0 を結ぶすべての極大鎖の長さは $d-1$, z_2 と 0 を結ぶすべての極大鎖の長さは $d-2$

であるから y_1, z_2 と0を結ぶ極大鎖は $d-1$ の長さを持つことになり，したがって鎖 $y_1>y_2>\cdots>0$ も $d-1$ の長さを持つ．ゆえに $x=y_0>y_1>\cdots>y_s=0$ も $d=s$ の長さを持つ．

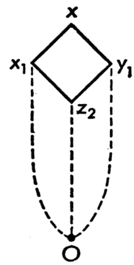


図 5. Jordan-Dedekind の条件

この定理により modular 束において成り立つ Jordan-Dedekind の条件をうる．

Jordan-Dedekind の条件： 二元を結ぶ有限な極大鎖がすべて同じ長さを持つ．

もし $a\supset b$ とすると b を商束 a/b における零元とみなせるから定理が適用される．

modular 束においては次元について次の重要な関係が成り立つ．

定理 8.3.3. 有限次元を持つ元からなる束において

$$d(x)+d(y)=d(x\cup y)+d(x\cap y)$$

が成立するための必要十分条件は束が modular 束となることである．

証：modular 束においては商 $x\cup y/x$, $y/x\cap y$ は同型であってそれぞれの中での有限極大鎖の長さは $d(x\cup y)-d(x)$, $d(y)-d(x\cap y)$ である．したがってこの二つの長さが等しいことから

$$d(x)+d(y)=d(x\cup y)+d(x\cap y) \tag{M}$$

をうる．

逆に束において(M)が成立するとする．$A\supseteq B$ と仮定して二元 $A\cap(B\cup C)$, $B\cup(A\cap C)$ を考える．

$$B\subseteq A,$$
$$B\subseteq B\cup C,$$
$$B\subseteq A\cap(B\cup C),$$
$$A\cap C\subseteq A,$$
$$A\cap C\subseteq C\subseteq B\cup C,$$
$$A\cap C\subseteq A\cap(B\cup C),$$
$$B\cup(A\cap C)\subseteq A\cap(B\cup C)$$

が成り立つから次元が等しいことを示せば二元が等しいことになる．(M) を使うと

$$
\begin{aligned}
d[B\cup(A\cap C)] &= d(B)+d(A\cap C)-d(B\cap A\cap C)\\
&= d(B)+d(A\cap C)-d(B\cap C)\\
&= d(B\cup C)-d(C)+d(A\cap C)\\
&= d(B\cup C)+d(A)-d(A\cup C)\\
&= d(A)+d(B\cup C)-d(A\cup B\cup C)\\
&= d[A\cap(B\cup C)]
\end{aligned}
$$

が成り立つから $A\cap(B\cup C)=B\cup(A\cap C)$ が得られ modular 束になる．

直後関係 $A>B$ によって，束において成立しうる**半 modular 律**の二つの性質を定義する．

定　義．下向きの半 modular 律：束において $A>B$, $A>C$, $B\neq C$ ならば $B>B\cap C$, $C>B\cap C$ が成立するときこの束を下向きの半 modular 束という．

上向きの半 modular 律：束において $A<B$, $A<C$, $B\neq C$ ならば $B<B\cup C$, $C<B\cup C$ が成立するときこの束を上向きの半 modular 束という．

明らかに半 modular 律の二つの性質は互いに双対的であって定理 8.3.1 により modular 束においては二つの性質は成り立っている．有限次元の束においては二つの半 modular 律から modular 律が得られることを示そう．

定理 8.3.4. 半 modular 束 L において $A\supseteq B$ であって A と B を結ぶ有限な極大鎖が存在すれば A と B を結ぶ有限な極大鎖の長さはすべて等しい．

証：証明は定理 8.3.2 の証明と本質的には同じである．L を下向きの半 modular 束とする．もし A と B を結ぶ長さ 1 の極大鎖があれば $A>B$ であって，これ以外に A と B を結ぶ鎖はない．A と B を結ぶ極大鎖の長さに関する帰納法で示すため

$$A=A_0>A_1>\cdots>A_r=B$$

を長さ r の極大鎖とし長さが r より小さい鎖については定理が成立していると仮定する．

$$A=U_0>U_1>U_2>\cdots>U_s=B$$

を別の A と B を結ぶ極大鎖とする．もし $U_1=A_1$ であれば帰納法の仮定により $A_1=U_1$ と B を結ぶ極大鎖の長さは $r-1$ であるから定理は成立する．$U_1\neq A_1$ のときは下向きの半 modular 律により

$$A_1>U_1\cap A_1,\quad U_1>U_1\cap A_1$$

が成り立つから $U_1\cap A_1=V_2$ とかくと次の鎖をうる．

$$A=A_0>A_1>A_2>\cdots>A_r=B,$$
$$A=A_0>A_1>V_2>\cdots>V_m=B,$$
$$A=U_0>U_1>V_2>\cdots>V_m=B,$$
$$A=U_0>U_1>V_2>\cdots>U_s=B.$$

A_1 と B を結ぶ鎖に関する帰納法の仮定により $m=r$ が得られ，したがって初めの二つの鎖の長さは同じになる．第二，第三の鎖の長さはともに m であって U_1 と B を結ぶ鎖に関する帰納法の仮定により $m=s$ が得られる．したがって四つの鎖はすべて同じ長さを持つことになり下向きの半 modular 束に対して定理の成立が示された．双対的議論により上向きの半 modular 束についても同じ結果が得られる．

この定理から半 modular 束においては元 A の次元 $d(A)$ は A と 0 を結ぶ任意の極大鎖の長さは等しいことが分かる．有限次元の半 modular 束においては次元函数について次の不等式が成立する．

定理 8.3.5. Lを有限次元の束とする．もしLが上向きの半 modular 束であれば，(1) $d(X\cup Y)+d(X\cap Y)\leqq d(X)+d(Y)$ が成立する．またLが下向きの半 modular 束であれば，(2) $d(X\cup Y)+d(X\cap Y)\geqq d(X)+d(Y)$ が成立する．逆に (1) は上向きの半 modular 律を意味するが，(2) からは下向きの半 modular 律は得られない．

証：定理 8.3.4 によりLが半 modular 束であって $R\supset S$ とするとRと 0

を結ぶ任意の極大鎖の長さは等しいから $d(R)-d(S)$ はRとSを結ぶ極大鎖の長さを与える．したがってRの次元はRと0を結ぶ極大鎖でSを含むものの長さに等しい．このことを使って定理の証明をする．

Lを上向きの半 modular 束とする．$A=B$ か $A>B$ のとき $A\geqq B$ とかいて "AはたかだかBの直後にしかない" と読むことにする．このときもし

$$X\cap Y=U_0<U_1<U_2<\cdots<U_m=X,$$
$$X\cap Y=V_0<V_1<V_2<\cdots<V_n=Y$$

であれば，$i=1,\cdots,m$；$j=1,\cdots,n$ に対し $U_i\cup V_j\geqq U_{i-1}\cup V_j$, $U_i\cup V_j\geqq U_i\cup V_{j-1}$ が成立することを $i+j$ に関する帰納法で示そう．まず $i+j$ の最小値2に対しては上向きの半 modular 律によって

$$U_1\cup V_1\geqq U_1=U_1\cup V_0,\quad U_1\cup V_1\geqq V_1=U_0\cup V_1$$

が成り立つ．また $U_i\cup V_j=(U_i\cup V_{j-1})\cup(U_{i-1}\cup V_j)$ であって帰納法の仮定から $U_i\cup V_{j-1}\geqq U_{i-1}\cup V_{j-1}, U_{i-1}\cup V_i\geqq U_{i-1}\cup V_{j-1}$ が成り立つから上向きの半 modular 律により $U_i\cup V_j\geqq U_i\cup V_{j-1}$, $U_i\cup V_j\geqq U_{i-1}\cup V_j$ が成立する．$j=n$ と置くと $V_n=Y$ であるから

$$Y\leqq U_1\cup Y\leqq U_2\cup Y\leqq\cdots\leqq U_m\cup Y=X\cup Y$$

が成立することになり $X\cup Y$ と Y を結ぶ極大鎖の長さはたかだかmとなる．したがって

$$d(X\cup Y)-d(Y)\leqq m=d(X)-d(X\cap Y)$$

から上向きの半 modular 束では不等式（1）が成立する．双対的議論により下向きの半 modular 束においては不等式（2）が成立する．したがって定理の前半が示された．後半を示すためにまず次の補題を証明しよう．

補題 8.3.1. Lにおいて不等式（1）が成立すれば $U>V$ は $d(U)=d(V)+1$ なることを示す．

証：$0=U_0<U_1<U_2<\cdots<U_{t-1}<U_t=U$ をUと0を結ぶ最長鎖とすると U_i と0を結ぶ i より長い鎖は存在しないから $d(U)=t$, $d(U_i)=i$ が $i=0,\cdots,t-1$ に対して成立する．また仮定から $U>V$ であるから $d(U)\geqq d(V)+1$ が

得られ，したがって $t-1 \geqq d(V)$ が成立する．さて $U_j \subseteq V$，$U_{j+1} \nsubseteq V$ なる U_j を選ぶ．そのような j は $0, 1, \cdots, t-1$ の中に必ずある．このとき $U_{j+1} \cup V = U$，$U_{j+1} \cap V = U_j$ であって不等式（1）から $d(U_{j+1} \cup V) + d(U_{j+1} \cap V) \leqq d(V) + d(U_{j+1})$ が成立する．すなわち $t+j \leqq d(V)+j+1$，あるいは $t-1 \leqq d(V)$ が成立する．したがって $d(V)=t-1$ となり $d(U)=t=d(V)+1$ が成立する．

この補題と不等式（1）から L が上向きの半 modular 束であることを示そう．$A<B$，$A<C$，$B \neq C$ と仮定すると $A=B \cap C$ であって $d(B)=d(A)+1$，$d(C)=d(A)+1$ が成り立つ．不等式（1）から $d(B \cup C)+d(B \cap C) \leqq d(B)+d(C)$ が成立するがこれは $d(B \cup C) \leqq d(A)+2$ なることを示す．一方 $B \cup C \neq B, C$ である．したがって $d(B \cup C)=d(B)+1=d(C)+1$ が成立しこれから $B \cup C > B$，$B \cup C > C$ が得られ，L は上向きの半 modular 束となる．次元 $d(X)$ は X と 0 を結ぶ最長鎖の長さとして定義されていて双対的な性質は持っていないから，不等式（2）からは L が下向きの半 modular 束なることはいえない．たとえば $A_1 \cap B_1 = A_1 \cap B_2 = 0$，$A_1 \cup B_1 = A_1 \cup B_2 = T$ なる関係を持つ五元 $0, T, A_1, B_1 \subset B_2$ からなる束は不等式（2）を満たすが下向きの半 modular 束ではない．

定理 8.3.6. 有限次元の束が modular 束であるための必要十分条件はその束が上向きの半 modular 束であって，かつ下向きの半 modular 束でもあることである．

証：modular 律から二つの半 modular 律が得られることはすでにみた．一方両向きの半 modular 律が成立するとすれば定理 8.3.5 から $d(X \cup Y) + d(X \cap Y) = d(X) + d(Y)$ が成立し，したがって定理 8.3.3 により modular 律が成立することになる．

定理 8.3.7. 有限 p 群の部分群全体は下向きの半 modular 束をなす．

証：群の部分群全体の集合は包含関係により部分順序集合となるから §1.4

で定義した部分群の和および積は束の公理を満たしている．有限 p 群の部分群 A, B, C において $A>B$, $A>C$ が成立するとすれば B, C はともに A の極大部分群ゆえ定理 4.3.2 から A に対する指数はともに p である．しからば定理 1.5.5 から $[B:B\cap C]$, $[C:B\cap C]$ はともに p 以下となるから 1 または p に等しくなる．したがって $B\neq C$ とすると $B>B\cap C$, $C>B\cap C$ が成立する．

8.4. 主組成列と組成列

前節で得られた結果を使って群の部分群の構造を調べることにする．群 G の部分群の列

(8.4.1) $$G=A_0\supseteq A_1\supseteq A_2\supseteq\cdots\supseteq A_n$$

で各部分群 A_i は直前の群 A_{i-1} の正規部分群なるものを考え A_i が A_{i-1} の正規部分群なることを

(8.4.2) $$A_i\lhd A_{i-1},\quad i=1,\cdots,n$$

とかき，また群 A_i を G の**部分正規群** (subinvariant group) という．この列から剰余群の列

(8.4.3) $$A_{i-1}/A_i,\quad i=1,\cdots,n$$

が得られる．

各 A_i が G の正規部分群であるとき列 (8.4.1) を**不変列** (normal series or invariant series) という．$i=1,\cdots,n$ に対して $A_i\lhd A_{i-1}$ であっても一般には $A_i\lhd G$ は成立しないから不変列の条件は (8.4.2) より強い．(8.4.2) だけを仮定するときこの列を**正規列***) (subinvariant series) という．各 A_i が A_{i-1} の極大正規部分群であるような不変列を**主組成列** (principal series or chief series) という．また各 A_i が A_{i-1} の極大正規部分群である正規列を**組成列** (composition series) という．束の言葉では (8.4.1) が含むという関係のとき不変列を主組成列，正規列を組成列という．作用団 Ω に関して A_i が認容部

*) Irving Kaplansky は正規列をもっと鮮明なる言葉で定義するように勧められたが，不必要な混乱をさけるため上のような定義とした．

分群なることを要求することもある.

modular 束に関する定理は, ある群の部分群についての定理, ループに関する合同関係についての定理, 合同関係が可換なる代数系の合同関係についての定理等とみなされる. 群について最も強い結果を与える主定理は定理 2.4.1 である. 束における諸定理は modular 律をもとにしているから代数系では種々の形でいい表わされる. 代数系の条件をいろいろ変えることにより束に関する一つの定理から異なった定理が得られる. 群においては modular 律に関する補助定理が必要とされる. 群Gの二つの部分群 A, B が集合として $AB=BA$ を満たすとき**交換可能である**という. このとき $A\cup B=AB=BA$ なることは明らかであるから集合 $AB=BA$ は部分群をなす. 定理 2.3.3 から部分群 A, B はどちらか一方が $A\cup B$ の正規部分群なるとき, しかもそのときに限り交換可能である.

定理 8.4.1. A, B, C を群Gの部分群であって $A\supseteq B$ とすると

$$A\cap(B\cup C)=B\cup(A\cap C)$$

が成立するためには B, C が交換可能なることは十分条件である.

証: 定理 8.3.3 の証明の途中におけると同じようにして $A\supseteq B$ ならば常に

$$B\cup(A\cap C)\subseteq A\cap(B\cup C)$$

が成立することが分かる. したがって逆向きの包含関係の成立を示せばよい. B, C は交換可能ゆえ $B\cup C$ の元は bc, $b\in B$, $c\in C$, とかけ $A\cap(B\cup C)$ の元はAおよび $B\cup C$ の元であるから $a=bc$, $a\in A$ と表わされる. $B\subseteq A$ から $c=b^{-1}a\in A$ が成り立つ. したがって $c\in A\cap C$ から $bc\in B\cup(A\cap C)$ となり $A\cap(B\cup C)\subseteq B\cup(A\cap C)$ が成立し定理が示されたことになる. この定理は B, C の可換性が $B\cup C=BC$ を意味するような逆元を持つループの部分ループについても成立する. それは $b^{-1}a=b^{-1}(bc)=c$ の成立が逆元の存在のみを要求するからである.

定理 8.4.2. 細分定理*⁾. $U=A_0\supseteq A_1\supseteq\cdots\supseteq A_n=V$, $U=B_0\supseteq B_1\supseteq\cdots\supseteq B_m=V$ を modular 束におけるUとVを結ぶ二つの有限鎖とする．そのとき $A_{i-1}=A_{i,0}\supseteq A_{i,1}\supseteq A_{i,2}\supseteq\cdots\supseteq A_{i,m}=A_i$, $i=1,\cdots,n$, $B_{j-1}=B_{j,0}\supseteq B_{j,1}\supseteq B_{j,2}\supseteq\cdots\supseteq B_{j,n}=B_j$, $j=1,\cdots,m$ であって商 $A_{i,j-1}/A_{i,j}$ と $B_{j,i-1}/B_{j,i}$ が射影的であるような元を挿入して両鎖を細分することができる．

証：$i=1,\cdots,n$, $j=1,\cdots,m$ に対し $A_{i,j}=A_i\cup(A_{i-1}\cap B_j)$, $B_{j,i}=B_j\cup(B_{j-1}\cap A_i)$ と置くと $A_{i,j-1}/A_{i,j}$ は

(8.4.4) $$A_{i-1}\cap B_{j-1}/(A_{i-1}\cap B_j)\cup(A_i\cap B_{j-1})$$

に射影され，$B_j\subseteq B_{j-1}$ から

(8.4.5) $$(A_{i-1}\cap B_{j-1})\cup A_i\cup(A_{i-1}\cap B_j)=A_i\cup(A_{i-1}\cap B_{j-1})$$

が成立する．また modular 律を使って

(8.4.6) $$\begin{aligned}&(A_{i-1}\cap B_{j-1})\cap[A_i\cup(A_{i-1}\cap B_j)]\\&=(A_{i-1}\cap B_j)\cup(A_{i-1}\cap B_{j-1}\cap A_i)\\&=(A_{i-1}\cap B_j)\cup(A_i\cap B_{j-1})\end{aligned}$$

が得られる．同様に $B_{j,i-1}/B_{j,i}$ は (8.4.4) の商に射影されるから定理が示されたことになる．

この定理と証明はGが作用域Ωを持つ群であれば部分群がすべて認容部分群であるときのGの正規列に対しても成立する．したがってΩとして恒等作用子のみからなるものを取れば作用域を持たない群についてもこの定理が成立する．

定理 8.4.3.（群の細分定理）. Gを作用域Ωを持つ群，$G=A_0\supseteq A_1\supseteq\cdots\supseteq A_n=H$, $G=B_0\supseteq B_1\supseteq\cdots\supseteq B_m=H$ をGとHを結ぶ認容部分群からなる二つの正規列とする．そのとき

---

*⁾ 最初の Jordan-Hölder の定理は多くの人により拡張されかつ一般化されてきた．最初の定理は C. Jordan [1], O. Hölder [1] により得られた．作用域を持つ群への一般化は E. Noether [1] と W. Krull [1, 2] によりなされた．細分定理は O. Schreier [4], H. Zassenhaus [1] により得られた．ここに与えられた束論による形式化は O. Ore [2] により与えられたものの修正である．部分順序集合への一般化は O. Ore [1], S. MacLane [3] によりなされた．

$$A_{i-1}=A_{i,0}\supseteq A_{i,1}\supseteq\cdots\supseteq A_{i,m}=A_i,\quad i=1,\cdots,n,$$
$$B_{j-1}=B_{j,0}\supseteq B_{j,1}\supseteq\cdots\supseteq B_{j,n}=B_j,\quad j=1,\cdots,m$$

であって商群

$$A_{i,j-1}/A_{i,j},\quad B_{j,i-1}/B_{j,i}$$

が作用同型となるような認容部分正規群を挿入することにより両鎖を細分することができる．

証：認容部分群の転置される（したがって射影される）商群は互いに作用同型である．したがって定理 8.4.2 の証明によりこの定理の証明が与えられることを示すには商群 X/Y が考えられることすなわち $Y\triangleleft X$ なることと (8.4.6) で modular 律が使えることを示さねばならない．認容部分群の和および共通部分はともに認容部分群であるから証明に現われる部分群はすべて認容的である．$A_i, A_{i-1}\cap B_j$ はともに $A_{i-1}\cap B_{j-1}$ により自分自身に変換されるから $A_{i,j}=A_i\cup(A_{i-1}\cap B_j)$ は $A_{i,j-1}=A_i\cup(A_{i-1}\cap B_{j-1})$ の正規部分群である．同様にして $B_{j,i}\triangleleft B_{j,i-1}$ が成立する．$A_{i-1}\cap B_j, A_i\cap B_{j-1}$ は $A_{i-1}\cap B_{j-1}$ の正規部分群であるから和も正規部分群となり，したがって (8.4.4) は確かに商群である．A_i は A_{i-1} の中で正規であるから A_i は A_{i-1} の任意の部分群と交換可能であり，したがって特に $A_{i-1}\cap B_j$ と交換可能である．ゆえに定理 8.4.1 から modular 律が使えて (8.4.6) が成立することになりこの定理が証明されたことになる．

主組成列および組成列においては（作用域の有無にかかわらず）これ以上の細分は不可能であって細分定理の直接の帰結として次の定理をうる．

定理 8.4.4. Jordan-Hölder の定理. $G=A_0\supset A_1\supset\cdots\supset A_n=H$, $G=B_0\supset B_1\supset\cdots\supset B_m=H$ を作用域 Ω を持つ二つの主組成列（または組成列）とすると $m=n$ であって商群 A_{i-1}/A_i は適当な順序で商群 B_{j-1}/B_j と作用同型となる．

$m=n$ は細分定理に現われる商群で単位群でないものの間の一対一対応から得られる．

不変列の場合正規部分群はすべて内部自己同型 $x \to a^{-1}xa$ の下で認容的であるから作用団Ωの中に内部自己同型全体を含ませることができる．内部自己同型全体を作用子に持つ同型写像は**中心同型写像**（central isomorphism）と呼ばれる．しからば細分定理から次の定理が得られる．

定理 8.4.5. 不変列の細分において対応する商群は中心同型である．

さて $x \to (x)\alpha$ をある群の中心自己同型とすると

$$a^{-1}(x)\alpha a = (a^{-1}xa)\alpha = (a)\alpha^{-1}(x)\alpha(a)\alpha$$

から $(a)\alpha a^{-1}$ はすべての $(x)\alpha$ と可換となり群の中心に含まれる．この元を z とかくと中心自己同型に対し群の任意の元 a と，a により定まる中心の元 z により $(a)\alpha = az$ が成立する．逆にこのような形の自己同型は中心自己同型なることが容易に示される．

8.5. 直 積 分 解

modular 束において m 個の元 $A_1, \cdots, A_m$ で，$i=1, \cdots, m$ に対し $\bar{A}_i = A_1 \cup \cdots \cup A_{i-1} \cup A_{i+1} \cup \cdots \cup A_m$ と置くと $A_i \cap \bar{A}_i = 0$（零元）となるものを考える．このとき $A = A_1 \cup \cdots \cup A_m$ を $A_1, \cdots, A_m$ の**直積**（direct union）といって

(8.5.1)
$$A = A_1 \times A_2 \times \cdots \times A_m$$

とかく．

定理 8.5.1.（**Ore の定理**）L を有限次元の任意の modular 束とする．L の全元 T が，直積分解不能な A_i, B_j に対して二つの分解 $T = A_1 \times \cdots \times A_m$，$T = B_1 \times \cdots \times B_n$ を持つとすれば $m = n$ であって A_i と B_j は適当な順序で射影的である．

証：任意に与えられた A，たとえばそれを A_1 とすると A_1 と射影的である B_j により置き換えられることをすなわち $T = A_1 \times A_2 \times \cdots \times A_m = B_j \times A_2 \times \cdots \times A_m$ となることを示そう．これがこの定理の主要部分である．A_1 が B_j で置き換えられたとすると，さらに第二の分解においてある B_k' で A_2 を置き換

える．置き換えの過程で同じ B_j が二度使われることはない．なぜならばもし二度使えたとすれば任意の因子は残りの因子の和との共通部分が0となることに反するからである．すべての A_i を置き換えるだけの B_j がなければならず $B_j \subseteq T$ から A_i をすべて置き換えた後には残りはなくなることになり $m=n$ が成り立つ．$\bar{A}_i = A_1 \cup \cdots \cup A_{i-1} \cup A_{i+1} \cup \cdots \cup A_m$, $i=1, \cdots, m$, $\bar{B}_j = B_1 \cup \cdots \cup B_{j-1} \cup B_{j+1} \cup \cdots \cup B_n$ と置き T の次元に関する帰納法で証明する．まず次元が1のときこの定理の成立は明らかである．

Case 1. ある j に対し $A_1 \cup \bar{B}_j = \bar{A}_1 \cup B_j = T$ となる．

$$\begin{aligned} d(A_1) &= d(T) - d(\bar{B}_j) + d(A_1 \cap \bar{B}_j) \\ &= d(B_j) + d(A_1 \cap \bar{B}_j) \geqq d(B_j) \end{aligned}$$

が成立し，同様に $d(B_j) \geqq d(A_1)$ も成立し，したがって $d(A_1) = d(B_j)$ が得られる．このことから $d(A_1 \cap \bar{B}_j) = d(\bar{A}_1 \cap B_j) = 0$ が成立し，$T = A_1 \times \bar{B}_j = \bar{A}_1 \times B_j$ が成り立ち A_1, B_j を互いに置き換えることができる．

Case 2. ある j に対し（たとえば $j=1$ とする）$A_1 \cup \bar{B}_j \subset T$ が成立する．

$h=1, \cdots, n$ に対し $D_h = A_1 \cup \bar{B}_h$, $Q_h = D_h \cap B_h$ と置く．もし $D_1 = A_1 \cup \bar{B}_1 \supseteq B_1$ とすると $D_1 \supseteq \bar{B}_1 \cup B_1 = T$ となり，仮定に反する．したがって $Q_1 = D_1 \cap B_1 \subset B_1$ であって $d(Q_1) < d(B_1)$ が成立する．T は B の直和であって $Q_h \subseteq B_h$ が $h=1, \cdots, n$ に対して成立するから Q の積は直積である．

$$C = \bigcup_{h=1}^{n} Q_h$$

と置くと T, C はともに直積であって $Q_1 \subset B_1$, $d(T) = d(B_1) + \cdots + d(B_n)$ から

$$d(C) = d(Q_1) + \cdots + d(Q_n) < d(T) \tag{8.5.2}$$

が成立する．

C は T に真に含まれているから次元に関する帰納法により C に対しては定理は成立する．$U_r = Q_1 \cup \cdots \cup Q_r$ と置いたとき，$M_r = B_1 \cup \cdots \cup B_r$, $N_r = D_1 \cap \cdots \cap D_r$ に対して $U_r = M_r \cap N_r$ なることを示そう．$r=1$ のときは定義 $U_1 = Q_1$ から $U_1 = B_1 \cap D_1$ となり，確かに成立しているから帰納法によって示すこと

にする．$U_j=M_j\cap N_j$ とすると $U_{j+1}=U_j\cup Q_{j+1}=(M_j\cap N_j)\cup(B_{j+1}\cap D_{j+1})$ が成立する．ここに $D_{j+1}\supseteq\bar{B}_{j+1}\supseteq M_j\supseteq M_j\cap N_j$ であるから modular 律により $U_{j+1}=D_{j+1}\cap[(M_j\cap N_j)\cup B_{j+1}]$ が成り立つ．また $B_{j+1}\subseteq\bar{B}_h\subseteq D_h$ が $h=1,\cdots,j$ に対して成立するから $B_{j+1}\subseteq N_j$ が成立し，したがって $U_{j+1}=D_{j+1}\cap[N_j\cap(B_{j+1}\cup M_j)]=N_{j+1}\cap M_{j+1}$ が得られて $U_r=M_r\cap N_r$ が成立することになる．$r=n$ のとき $M_r=T$ であって $h=1,\cdots,n$ に対し $D_h\supseteq A_1$ なることから

(8.5.3) $$C=Q_1\cup\cdots\cup Q_n=D_1\cap\cdots\cap D_n\supseteq A_1$$

が成立する．$C\supseteq A_1$ であるから modular 律を使って $(C\cap\bar{A}_1)\cup A_1=C\cap(\bar{A}_1\cup A_1)=C\cap T=C$ が成立する．$C\cap\bar{A}_1\cap A_1=0$ は明らかであるから

(8.5.4) $$C=A_1\times(C\cap\bar{A}_1)=Q_1\times\cdots\times Q_n$$

が成り立つ．Cについてはこの定理は成立しているから A_1 を，あるQの分解不能な因子（それを $E\subseteq Q_h$ とする）で置き換えられる．置き換えが可能なることから $d(E)=d(A_1)$ であり，また $C=E\times(C\cap\bar{A}_1)$ から $0=E\cap C\cap\bar{A}^1=E\cap\bar{A}_1$ でもある．したがって $d(E\cup\bar{A}_1)=d(E)+d(\bar{A}_1)=d(A_1)+d(\bar{A}_1)=d(T)$ から $T=\bar{A}_1\cup E=E\times\bar{A}_1$ が成立する．さらに $E\subseteq Q_h=(A_1\cup\bar{B}_h)\cap B_h\subseteq B_h$, $E\cap(\bar{A}_1\cap B_h)=E\cap\bar{A}_1=0$ から modular 律を使って $E\cup(\bar{A}_1\cap B_h)=B_h\cap(E\cup\bar{A}_1)=B_h\cap T=B_h$ が得られ，したがって

(8.5.5) $$B_h=E\times(\bar{A}_1\cap B_h)$$

が成り立つ．

一方仮定から B_h は分解不能であり $d(E)=d(A_1)>0$ であるから $B_h=E$, $\bar{A}_1\cap B_h=0$ である．このことは

(8.5.6) $$T=A_1\times\bar{A}_1=B_h\times\bar{A}_1$$

なることを示している．また $B_h=E\subseteq Q_h\subseteq B_h$ から $B_h=Q_h=(A_1\cup\bar{B}_h)\cup B_h$ が成り立つ．すなわち $B_h\subseteq A_1\cup\bar{B}_h$ が成り立つから，$A_1\cup\bar{B}_h\supseteq B_h\cup\bar{B}_h=T$ が成り立つことになる．$d(A_1)=d(B_h)$ であるから，$d(A_1\cap\bar{B}_h)=d(A_1)+d(\bar{B}_h)-d(A_1\cup\bar{B}_h)=d(B_h)+d(\bar{B}_h)-d(T)=0$ が成り立ち，したがって

(8.5.7) $$T=A_1\times\bar{B}_h$$

が成立することになり A_1, B_h は互いに置き換えることができる．ここに $A_1\cup\bar{B}_h=T$，$A_1\cup\bar{B}_1\neq T$ から $h\neq 1$ である．

Case 3. Case 1, 2 でない，すなわちすべての j に対し $A_1\cup B_j=T$ であって，かつ $A_1\cup B_j\subset T$ である．

A, B の役割を入れ換えることにより Case 2 が適用されるから任意に選ばれた B（それを B_n とする）は A_1 と異なるある A（番号を付け換えることにより，A_m であるとしてよい）と互いに置き換えることができる．したがって

$$T=A_1\times\cdots\times A_{m-1}\times A_m \\ =B_1\times\cdots\times B_{n-1}\times A_m=\bar{B}_n\times A_m \tag{8.5.8}$$

が成立する．ここに $z\to(z\cup A_m)\cap\bar{A}_m$ は商 $\bar{B}_n/0$ から商 $\bar{A}_m/0$ の上への射影であるから，定理 8.3.1 の系により束同型である．よって $j=1,\cdots,n-1$ に対して $B_j{}^*=(B_j\cup A_m)\cap\bar{A}_m$ と置くと同型なることから

$$\bar{A}_m=A_1\times\cdots\times A_{m-1}=B_1{}^*\times\cdots\times B_{n-1}{}^* \tag{8.5.9}$$

が成立する．次元に関する帰納法の仮定により $\bar{A}_m$ に対しては定理が成立するから，A_1 はある $B_j{}^*$（それを $B_1{}^*$ とする）で置き換えられる．したがって $B_1\cup A_m=(B_1\cup A_m)\cap(\bar{A}_m\cup A_m)=[(B_1\cup A_m)\cap\bar{A}_m]\cup A_m=B_1{}^*\cup A_m$ であるから $B_1\cup\bar{A}_1=(B_1{}^*\cup A_2\cup\cdots\cup A_{m-1})\cup A_m=(A_1\cup A_2\cup\cdots\cup A_{m-1})\cup A_m=T$ が成立する．一方 $A_1\cup\bar{B}_1=T=B_1\cup A_1$ であるから Case 1 が適用できて A_1 と B_1 は互いに置き換えられることになる．Case 3 は実際には起こりえないこと，および与えられた A_1 に対しどの場合でも A_1 と B_j が互いに置き換えられるような B_j が存在することを注意しておこう．

群に対してはこの定理は次のようになる．

定理 8.5.2.（**Wedderburn-Remak-Schmidt の定理***⁾）．Gをその正規部分群が有限次元の束をなすような群とする．そのときGが次のように分解不能な部

*⁾ この定理をはじめて証明したのは T. H. M. Wedderburn [1] である．R. Remak [1, 2] はその不備を補い，P. Schmidt は作用域を持つ群にまでそれを拡張した．束についての定理 (8.5.1) は Ore [1] により示されたがここに与えられた形は G. Birkhoff [1] のものを少し変えたものである．

分群の直積として二通りに表わされるとすれば

$$G=A_1\times\cdots\times A_m,$$
$$G=B_1\times\cdots\times B_n,$$

$m=n$ であってどの A_i もある B_j と互いに置き換えることができて，かつそのような A_i と B_j は中心同型である．この定理は作用域を持つ群，逆元を持つループの合同関係に対しても成立する．

証：正規部分群全体が modular 束をなすことはすでにみたから，直積の次元が一致することを示せば十分である．$G=A_i\times\bar{A}_i=B_j\times\bar{A}_i$ において A_i, B_j はともに $G/\bar{A}_i$ に転置されるから射影的である．したがって A_i から B_j への中心同型が存在するから $\bar{A}_i$ は自分自身に写すと定義すれば，この中心同型はGの中心自己同型となる．ゆえに A_i の元に対応する B_j の元は A_i の元にGの中心の元を掛けたかたちで表わされる．

8.6. 群の組成列

$G=A_0\supset A_1\supset\cdots\supset A_n=H$ をGと部分群Hを結ぶ組成列とする．定義により A_{i+1} は A_i の極大正規部分群であって A_i/A_{i+1} の正規部分群に対し A_{i+1} を含む A_i の正規部分群が対応する（定理 2.3.4）から A_i/A_{i+1} は単純群である．したがってもし A_i/A_{i+1} が可換群であれば，真部分群を含み得ないから素数位数の単純群である．主組成列と組成列の間の関係が次の定理により与えられる．

定理 8.6.1. Hを，GとHを結ぶ組成列が存在するようなGの正規部分群とする．このときGとHを結ぶ主組成列

$$G=B_0\supset B_1\supset\cdots\supset B_m=H$$

で各商群 B_i/B_{i+1} が互いに同型な単純群の有限個の直積であるようなものが存在する．逆にそのような列が存在すればGとHを結ぶ組成列がある．

証：GとHを結ぶ任意の不変列は細分することにより組成列にできるから，

GとHを結ぶ任意の不変列は組成列より長くない．したがって有限の長さを持つことになる．よってGとHを結ぶ主組成列

$$G=B_0\supset B_1\supset\cdots\supset B_m=H$$

が存在する．もし $m=1$ とすると G/H は単純群であるから定理は成立する．したがってmについての帰納法で証明することにし各 $B_0/B_1, \cdots, B_{m-2}/B_{m-1}$ は同型な単純群の有限個の直積であると仮定する．このとき B_{m-1}/B_m が同型な単純群の有限個の直積なることを示せばよい．B_{m-1}/B_m の任意の正規部分群に対し B_m を含む B_{m-1} の正規部分群が対応しているから，$K\supset B_m$ であってKが B_{m-1} の正規部分群であるような B_{m-1}/B_m の極小正規部分群 K/B_m が存在する．$K=B_{m-1}$ であれば B_{m-1}/B_m は単純群であるから証明は終る．さてGの中でのKの共役 K_j を考えよう．B_{m-1} はGの正規部分群であるから $K_j\subseteq B_{m-1}$ が成立している．さらにGの元による変換は B_{m-1} の自己同型を引き起こすから各 K_j は B_{m-1} の正規部分群である．またGの元による変換により K_j の中に置換が起こるだけであるから $\bigcup_j K_j$ はGの正規部分群である．B_{m-1} と B_m の間にはGの正規部分群は存在しないから $\bigcup_j K_j=B_{m-1}$ が成立する．ここで $K=K_1$, $K_2\not\subseteq K_1$, $K_3\not\subseteq K_1\cup K_2, \cdots, K_j\not\subseteq K_1\cup\cdots\cup K_{j-1}$ となるように K_j を取ると各 $U_j=K_1\cup\cdots\cup K_j$ は B_{m-1} の正規部分群であって U_{j-1} を含む．Gと B_m を結ぶ組成列で B_{m-1} をその列に含むものがあるから U_j の個数は有限であって，ある有限な j に対し $B_{m-1}=U_j=K_1\cup\cdots\cup K_j$ となる．各 K_i は B_m を含む B_{m-1} の極小正規部分群であるから，K_i を残りのKの和に含まれないものとすると，K_i とその残りのKの和との共通部分は B_m に含まれることになる．したがって残りの和に含まれてしまうKを取り去ると $B_{m-1}/B_m=K_1/B_m\cup\cdots\cup K_s/B_m$ とかけ，各 K_i/B_m は B_{m-1}/B_m の正規部分群であって残りの和との共通部分は単位群である．このとき定理 3.2.2 から B_{m-1}/B_m は $K_1/B_m, \cdots, K_s/B_m$ の直積になる．もし K_1/B_m が真の正規部分群を持つとすれば，それは残りの直積因子により正規化されるから B_{m-1}/B_m の正規部分群である．しかるに K_1/B_m は B_{m-1}/B_m の極小正規部分群であった．ゆえに K_1/B_m は単純群であって B_{m-1}/B_m はそれら s 個の同型な単

純群の直積となる．

この定理の逆に対しては $B_m \subset K \subset U_2 \subset U_3 \subset \cdots \subset B_{m-1}$ が組成列の一部分となることから明らかである．なぜならば各商群は単純群だからである．

定理 8.6.2*)．群 G の二つの部分正規群の共通部分は G の部分正規群である．ある組成列に現われる二つの部分群の和および共通部分をともに含む組成列がある．

証：A, B を G の部分正規群とすると，定義から G の二つの鎖

$$A = A_r \lhd A_{r-1} \lhd \cdots \lhd A_1 \lhd G,$$
$$B = B_s \lhd B_{s-1} \lhd \cdots \lhd B_1 \lhd G$$

が存在する．鎖 $A = A_r \supseteq A_r \cap B_1 \supseteq \cdots \supseteq A_r \cap B_s = A \cap B$ において各部分群は直前の部分群に一致するか，その真の正規部分群である（定理 2.4.1）からこれらのうち異なる部分群を C_i で表わすことにすれば

$$A \cap B \lhd C_u \lhd C_{u-1} \lhd \cdots \lhd C_1 \lhd A_r \lhd \cdots \lhd A_1 \lhd G$$

となり $A \cap B$ は G の部分正規群となる．

さて，始めに与えた二つの鎖をともに組成列としよう．B_1 と A_1 は G の極大正規部分群であるから $B_1 \neq A_1$ ならば $G = A_1 \cup B_1$ である．$A_1 \cap B_1$ は G の正規部分群であり $A_1/A_1 \cap B_1 \cong G/B_1$ において右辺が単純群なることから，$A_1 \cap B_1$ は A_1 の極大正規部分群である．このとき $A_1 \cap B_1 = A_2$ であるか $A_1 \cap B_1$ と A_2 が A_1 の異なる二つの極大正規部分群であって，もし後者であれば $A_1 = A_2 \cup (A_1 \cap B_1)$，$A_2 \cap B_1 = A_2 \cap (A_1 \cap B_1)$ が成立し $A_2/A_2 \cap B_1 \cong A_1/A_1 \cap B_1 \cong G/B_1$ の右辺が単純群であって $A_1 \cap B_1/A_2 \cap B_1 \cong A_1/A_2$ が成立する．この操作を続けていけば $A = A_r = A_r \cap B_1$ であるか，または $A_r \cap B_1 \lhd A_r$ であって $A_r/A_r \cap B_1 \cong G/B_1$ が単純群，のいずれかをうる．したがって組成列

$$A_r \cap B_1 \lhd A_{r-1} \cap B_1 \lhd \cdots \lhd A_1 \cap B_1 \lhd B_1 \lhd G,$$
$$B_s \lhd B_{s-1} \lhd \cdots \lhd B_2 \lhd B_1 \lhd G$$

---

*) この結果は H. Wielandt [2] による．

が得られる．B_1 の代りに B_2 を用いて上記の操作を繰り返し行なうことにより，最後にはGと $A\cap B$ を結ぶ組成列をつくることができる．

二つの組成群（組成列に現われる部分群を組成群ということにする）の和が組成群なることを示すのはより複雑である．Gと $A=A_r$ および $B=B_s$ を結ぶ組成列の長さ r と s に関する帰納法で，したがって特に $r+s$ に関する帰納法で示そう．$A_1\cup B_1$ はGの正規部分群であるから $r+s=2$ のとき定理は成立する．証明には次の補題が必要である．

補題 8.6.1. 組成群Aを真部分群として含むGの組成群をCとすればGとAを結ぶ組成列でCが現われるものがある．したがって特にGとCを結ぶ組成列の長さはGとAを結ぶ組成列の長さより小さい．

$$C=C_t \lhd C_{t-1} \lhd \cdots \lhd C_1 \lhd G,$$
$$A=A_r \lhd A_{r-1} \lhd \cdots \lhd A_1 \lhd G$$

をAとCに対する組成列とすれば前と同様にして

$$A_r=A_r\cap C_t \lhd A_{r-1}\cap C_t \lhd \cdots \lhd A_1\cap C_t \lhd C_t \lhd \cdots \lhd C_1 \lhd G$$

が成立するから C_t と A_r の間を異なる部分群のみを残せばGとAを結ぶ組成列が得られることになり，したがって $r>t$ が成立する．これで補題が証明された．

帰納法の仮定から $A_{r-1}\cup B_s$, $A_r\cup B_{s-1}$ はともにGの組成群である．もし $A_{r-1}\cup B_s$ がGの真部分群であれば A_r, B_s はともに $A_{r-1}\cup B_s$ の組成群で長さ r', s' は補題により，$r'<r$, $s'<s$ を満たす．したがって帰納法の仮定から $A_r\cup B_s$ は $A_{r-1}\cup B_s$ の組成群であり，したがってGの組成群でもある．したがって $A_{r-1}\cup B_s=G$ であると仮定してもよい．同様にして $A_r\cup B_{s-1}=G$ と仮定してもよい．対称性から $r<s$ とする．$B_s\ni b$ に対し A_1 はGの正規部分群であるから $b^{-1}A_1b=A_1$ が成立し，したがって

$$b^{-1}A_rb \lhd b^{-1}A_{r-1}b \lhd \cdots \lhd b^{-1}A_2b \lhd A_1 \lhd G$$

が成立する．もし $b^{-1}A_rb\neq A_r$ であるとすれば A_r と $b^{-1}A_rb$ は長さがともに $r-1$ の A_1 の組成群であるから，帰納法の仮定から $A^*=A_r\cup b^{-1}A_rb$ は

A_1 の組成群であって，A_1 と A^* を結ぶ鎖の長さは $r-1$ より小さい．したがって再び帰納法の仮定から $B_s\cup A^*$ は組成群である．$B_s\cup A^*=B_s\cup A_r=B\cup A$ であるから，B_s の各元による変換で A_r は自分自身に移されるとしてよい．A_r は A_{r-1} の正規部分群であるから A_r は $A_{r-1}\cup B_s=G$ の正規部分群となる．Gの正規部分群 A_1 として A_r を取ることができるから，このとき明らかに $B\cup A=B_s\cup A_1 \lhd B_{s-1}\cup A_1\lhd\cdots\lhd B_1\cup A_1\lhd G$ が成立する．したがってAを含む組成列における $B\cup A$ は組成群である．

演 習 問 題

1. Gを位数 p^rq^s の群とする．もしGが二つの組成列 $1\subset A_1\subset A_2\subset\cdots\subset A_r\subset A_{r+1}\subset\cdots\subset A_{r+s}=G$, $1\subset B_1\subset B_2\subset\cdots\subset B_s\subset B_{s+1}\subset\cdots\subset B_{s+r}=G$ を持ち，A_r の位数が p^r, B_s の位数が q^s であればGは A_r, B_s の直積であることを示せ．
2. 有限群Gの位数を割るすべての素数pに対し，p-Sylow 部分群を組成群に持つようなGの組成列があれば，Gが Sylow 部分群の直積となることを示すために問題1の結果を一般化せよ．
3. 有限個の非可換単純群の直積で表わされる群の自己同型は，各直積因子を入れ換えるだけである．
4. 有限生成の群Gが極大部分群Aをただ一つだけ含むときは，Aに含まれない任意のGの一元でGが生成されることを示せ．さらにGは素数巾の巡回群なることを示せ．
5. p, q を異なる素数とする．もし有限生成の群Gが $[G:A]=p$, $[G:B]=q$ なる極大部分群 A, B を丁度二つだけ含むとすれば，Gは位数 p^iq^j の巡回群なることを示せ．（ヒント：$A\cap B$ が正規部分群であって $G/A\cap B$ が巡回群なることを示せ．）
6. Gを $L(G)$ の次元が2の有限群とする．もしGの位数が平方数で割り切れないとすれば，正規部分群となるような Sylow 部分群が少なくとも一つ存在することを示せ．したがってこのことから p, q を素数としてGの位数が pq とかけることが分かる．

第9章　Frobenius の定理；可解群

9.1. Frobenius の定理

定理 9.1.1 はその原形を Frobenius [2] にみることができるが，群論の大部分の結果とは全く異なった性格を持っている．すなわち部分群，準同型，置換表現等の言葉ではなく，有限群におけるある方程式の解の個数でこの定理は述べられている． この定理は， 方程式論を一般化したことで知られる Philip Hall [3] によって大巾に一般化されたが， ここでは原形を少し一般化した形で述べる．

定理 9.1.1. Gを位数gの群，Cをh個の元からなるGの共役類とする． cがCの元全体をうごくとき $x^n=c$ の解の個数は (hn, g) の倍数である．

証： n乗が複体Kに含まれるようなGの元全体の集合を $A(K, n)$ で， また $A(K, n)$ に含まれる元の個数を $a(K, n)$ でそれぞれ表わすことにする．$g=1$ のときは $(hn, g)=1$ であるからこの定理は成立する． また $n=1$ のときも解の個数は $h=(h, g)$ であるから定理は成立する． したがって g, n に関する帰納法で証明するために，$g'<g$, $n'<n$ なるすべての g', n' について定理が成立しているとしよう．

もし $c'=u^{-1}cu$, $x^n=c$ とすると $(u^{-1}cu)^n=c'$ となるから，ある元cに対する解の集合とその任意の共役元に対する解の集合の間には一対一の対応が存在する． したがって $a(C, n)=a(c, n)\cdot h$ が成立する． またもし $x^n=c$ であれば $x^{-1}cx=x^{-1}x^nx=x^n=c$ となるから $x^n=c$ の解はcの正規化群 N_c に含まれ， 定理 1.6.1 から N_c の位数は g/h である． したがって $h>1$ なら N_c においては定理が成立することになり $a(c, n)$ は $(n, g/h)$ の倍数であるから $a(C, n)=a(c, n)\cdot h$ は $h(n, g/h)=(hn, g)$ の倍数となり定理が示されたこと

になる．したがって $h=1$ としてよい．またもし $n=n_1n_2$, $(n_1, n_2)=1$, $n_1>1$, $n_2>1$ と分解されたとすると，$D=A(c, n_2)$ と置くと $A(C, n)=A(D, n_2)$ であってDは完全共役類からなる．帰納法の仮定から (n_1, g) は $a(C, n)$ の約数であり，同様にして (n_2, g) も $a(C, n)$ の約数となる．しかるに (n_1, g) と (n_2, g) は互いに素であるから $(n_1, g)\cdot(n_2, g)=(n_1n_2, g)=(n, g)$ は $a(C, n)$ の約数となって定理が成立する．したがってnを素数巾 $n=p^e$ としてよい．もしpがcの位数uを割り切るとすれば，$A(c, n)$ には位数が nu なる元xがありxで生成される巡回群の中に，$A(c, n)$ に含まれる元が丁度n個ある．それらn個のどの元も同一の部分群を生成するから $a(c, n)$ はnで割り切れる．

よって $n=p^e$ と c の位数uが互いに素なる場合に定理を証明すればよい．$h=1$ であるからcはGの中心に含まれる．Gの中心の元で位数がpで割り切れないもの全体は可換群BをなしBの位数bはpと互いに素である．

さて c_1, c_2 をBの二元としよう．$p \nmid b$ であるから方程式 $c_2=c_1y^n$ はBにただ一つの解yをもつ．もし $x^n=c_1$ とすると $(xy)^n=c_2$ が成立するから各 $c\in B$ に対し $a(c, n)$ は一定である．したがって共役類CでBに含まれる元，含まれない元について $a(C, n)$ を計算することにより

$$g=\sum_{C\not\subset B}a(C, n)+b\cdot a(c, n)$$

が成立する．最初の和における各項 $a(C, n)$ は帰納法または証明の前半が使えて (n, g) で割り切れる．一方 (n, g) はgの約数であってbと互いに素であるから (n, g) は $a(c, n)$ を割り切らねばならない．よって証明は完結した．

cを単位元とすると $h=1$ であって Frobenius の定理の原形が得られる．ここにGの任意の元xに対し $x^g=1$ が成り立つから $(n, g)=m$ とすると $x^n=1$ なら $x^m=1$ が成立する．

定理 9.1.2. nが群Gの位数を割り切るならばGの中で $x^n=1$ の解の個数はnの倍数である．

単位元は $x^n=1$ を満たすから解の個数は少なくともn以上であることに注意しよう．

この定理と関連した興味深い次の予想がある．

もし n が群 G の位数を割り切り G の中で $x^n=1$ が丁度 n 個の解をもてば，それらの解全体は G の正規部分群をなす．

G が位数 n の部分群 H を持てば，H の元は方程式の解であり，また $x^n=1$ ならば任意の z に対し $(z^{-1}xz)^n=1$ が成立して，（解が丁度 n 個であれば）H は正規部分群となる．したがって問題は n 個の解全体が部分群 H をなすことを示すことにある．Lagrange の定理から部分群の位数が群の位数の約数なることから n が G の位数の約数であると仮定するのは本質的であろう．たとえば $x^4=1$ は3次の対称群の中にちょうど4個の解をもつが，3次対称群の位数は6であるから解全体は部分群をなさない．

9.2. 可　解　群

群 G の元 $x^{-1}y^{-1}xy$ は x と y の**交換子**（commutator）と呼ばれ $x^{-1}y^{-1}xy=(x,y)$ とかく．また $(x_1,\cdots,x_{n-1},x_n)=((x_1,\cdots,x_{n-1}),x_n)$ によって帰納的に高位の交換子を定義し，これらを**単純交換子**（simple commutator）と呼ぶ．より一般に交換子達の交換子を**複合交換子**（complex commutator）とよぶことにする．たとえば $((a,b),(c,d,e))$ は複合交換子である．帰納的に交換子の重さ ω を次のように定義する．G の元 g は重さ1とし $\omega(g)=1$ とかき，また交換子 (x,y) に対しては $\omega(x,y)=\omega(x)+\omega(y)$ と置く．しからば交換子の重さはその元の交換子としての表現により定まり群のどの元であるかには関係しない．

定義から $(x,y)=1$ と $yx=xy$ とは同値であるから G が可換群なるとき，しかもそのときに限り G のすべての交換子が1となる．したがって交換子は，ある群がどの程度可換性をもっているかを測る尺度とみられる．群 G の交換子 $x^{-1}y^{-1}xy$ 全体で生成される部分群 G' は**交換子群**（commutator subgroup）あるいは**導群**（derived subgroup）とよばれる．明らかに G' は G の全不変部分群である．

定理 9.2.1. 商群 G/G' は可換群である．もしKを G/K が可換群となるGの正規部分群とすれば $K\supseteq G'$ が成立する．

証：写像 $G\to G/G'=H$ においてHの任意の二元 u,v に対し $x\to u, y\to v$ とすると，$x^{-1}y^{-1}xy\to u^{-1}v^{-1}uv$ が成り立つ．一方 $x^{-1}y^{-1}xy\in G'$ であるから $x^{-1}y^{-1}xy\to 1=u^{-1}v^{-1}uv$ が，したがって $uv=vu$ が成立し，G/G' は可換群となる．次に G/K が可換群と仮定する．Gの元 x,y に対し，写像 $G\to G/K$ により $x\to u$，$y\to v$ であるとすれば，$x^{-1}y^{-1}xy\to u^{-1}v^{-1}uv=1$ が成立し，任意の交換子 $x^{-1}y^{-1}xy$ がKに含まれることになり $K\supseteq G'$ が成立する．

定　義：群Gの列 $G\supseteq G'\supseteq G''\supseteq\cdots\supseteq G^{(i)}\supseteq\cdots$，において $G^{(e)}=1$ となる e が存在するときGは可解群であるという．ただし各 $G^{(i)}$ は $G^{(i-1)}$ の交換子群とする．

定理 9.2.1 により各商群 $G^{(i)}/G^{(i+1)}$ は可換群である．もし $G^{(i)}=G^{(i+1)}$ となったとすると $j\geqq i$ なるすべての j に対して $G^{(i)}=G^{(j)}$ が成立することは明らかであるから定義の包含は $G^{(i)}=1$ が成立するまでは真の包含関係である．

定理 9.2.2. 可解群の任意の部分群および商群は可解群である．

証：Gを可解群，Hをその部分群とする．H' はHの元による交換子全体で生成された群であり，G' はGの元による交換子全体で生成された群であるから $H'\subseteq G'$ が成立する．したがって $H''\subseteq G''$, $H'''\subseteq G'''$, $\cdots$，が順次成立することになる．$G^{(e)}=1$ とすると $H^{(e)}=1$ となるからHは可解群である．もちろん $i<e$ なる i に対してすでに $H^{(i)}=1$ となることもある．次に $Q=G/K$ をGの商群として準同型 $G\to Q$ を考える．Qの各交換子はGの交換子の像であるから $G'\to Q'$ となる．この操作を続けていけば $G^{(e)}\to Q^{(e)}$ が得られるから $G^{(e)}=1$ であれば $Q^{(e)}=1$ が成り立ちQは可解群となる．このときも $i<e$ なるある i に対して $Q^{(i)}=1$ となっていることもありうる．

定理 9.2.3*). 有限群Gが可解群なるための必要十分条件はGと1を結ぶ組成列における商群が素数位数の巡回群なることである.

証：$G=A_0\supset A_1\supset\cdots\supset A_r=1$ において各 A_{i-1}/A_i, $i=1,\cdots,r$ が素数位数の巡回群とする. G/A_1 は可換群ゆえ定理 9.2.1 により $A_1\supseteq G'$ が成り立つ. 同様に $A_2\supseteq A_1'\supseteq G''$ が成立し以下続けていけば $A_r\supseteq G^{(r)}$ が成立することになり, したがって $G^{(r)}=1$ が得られるからGは可解群となる. 逆にGを有限可解群とすると G/G' は可換群であるから列

$$G\supset G'\supset G''\supset\cdots\supset G^{(e)}=1$$

において $A_1\supseteq G'$ なる極大正規部分群 A_1 が存在する. このとき G/A_1 は単純かつ可換ゆえ素数位数の巡回群である. 同様にして A_1 が可解群なることから A_1 は A_1/A_2 が素数位数の巡回群なる極大正規部分群 A_2 を含む. この操作を続けていけばGの列 $G=A_0\supset A_1\supset\cdots\supset A_r=1$ で各 A_{i-1}/A_i が素数位数の巡回群なるものが得られ Jordan-Hölder の定理からどの組成列についても同じことが成立する.

定理 9.2.4. 有限可解群Gの主組成列

$$G=C_0\supset C_1\supset\cdots\supset C_s=1$$

において各商群 C_{i-1}/C_i ($i=1,\cdots,s$) は基本可換群である.

証：定理 8.6.1 により C_{i-1}/C_i は同型な単純群のいくつかの直積であり, 定理 9.2.2 からこれらの単純群は可解群, したがって素数位数の巡回群である. ゆえに C_{i-1}/C_i は同じ素数位数pの巡回群の直積であるから基本可換群となる. 逆にそのような主組成列をGが持つとすれば商群はすべて可換群であるからGは可解群となる. $C_0/C_1,\cdots,C_{s-1}/C_s$ の位数 $c_1,\cdots,c_s$ をGの**主組成因子** (chief factors) という. 主組成因子は既に示したように素数巾である. 明らかに商群 G/K の主組成因子はGの主組成因子の部分集合である. なぜなら

---

*) 歴史的には組成列のこの性質が可解群の定義であったがこのような定義は無限群には適用されない. ガロアの理論は整方程式 $f(x)=0$ が代数的に解けること, すなわち可解なることと, そのガロア群が可解群なることが同値であることを示している.

正規部分群Kを含むGの主組成列が存在するからである．Gの部分群Hに対し

$$H \supseteq H \cap C_1 \supseteq H \cap C_2 \supseteq \cdots \supseteq H \cap C_s = 1$$

なる列の中で異なる部分群全体はHの不変列をなし，この列自身あるいはその細分がHの主組成列を与える．したがって $H \cap C_{i-1}/H \cap C_i$ が C_{i-1}/C_i の部分群と同型なることからHの主組成因子（の構成員）はGの主組成因子（のある構成員）の約数である．

定理 9.2.5. 群Gの次の二つの性質はともにGの可解性と同値である．

1） Gは有限不変列

$$G = A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots \supseteq A_s = 1$$

で各 A_{i-1}/A_i $(i=1, \cdots, s)$ が可換群となるようなものを持つ．

2） Gは有限正規列

$$G = B_0 \supseteq B_1 \supseteq B_2 \supseteq \cdots \supseteq B_t = 1$$

で各 B_{i-1}/B_i $(i=1, \cdots, t)$ が可換群となるようなものを持つ．

証：Gが可解群であれば，Gの交換子群列

$$G \supset G' \supset G'' \supset \cdots \supset G^{(r)} = 1$$

は各 $G^{(i-1)}/G^{(i)}$ $(i=1, \cdots, r)$ が可換群なる有限不変列であるから 1）が成立し，したがって特に 2）も成立する．2）から群Gの可解性が示されることをいえば十分である．$G = B_0 \supseteq B_1 \supseteq B_2 \supseteq \cdots \supseteq B_t = 1$ を B_{i-1}/B_i $(i=1, \cdots, t)$ が可換群なるGの正規列とすると $G/B_1 = B_0/B_1$ が可換群なることから $B_1 \supseteq G'$ が成り立つ．同様に $B_{i-1} \supseteq G^{(i-1)}$ とすると $B_i \supseteq B_{i-1}' \supseteq G^{(i)}$ が成り立つから $1 = B_t \supseteq G^{(t)}$ から $G^{(t)} = 1$ が成立しGは可解群となる．

系 9.2.1. 群Gが正規部分群Hを持ち $H, G/H$ がともに可解ならばGも可解である．

$G/H \supseteq A_1/H \supseteq \cdots \supseteq A_{r-1}/H \supseteq H/H,\ H \supseteq B_1 \supseteq \cdots \supseteq B_{s-1} \supseteq 1$をそれぞれ$G/H$, Hに対する 2）を満たす列とすると $G \supseteq A_1 \supseteq \cdots \supseteq A_{r-1} \supseteq H \supseteq B_1 \supseteq \cdots \supseteq B_{s-1} \supseteq 1$ はGに対して 2）を満たす列となる．

9.3. 可解群における拡張された Sylow の定理

有限群の Sylow 部分群は位数 $m=p^a$ と指数 n とが互いに素であるという性質を持っている．Philip Hall [1] は可解群において位数 m が指数 n と互いに素なる部分群の言葉で m が素数巾という仮定なしに Sylow の定理が一般化されることを示した．

定理 9.3.1. G を位数 mn の可解群で $(m,n)=1$ とすると

（1） G は少なくとも一つ位数 m の部分群を含む．

（2） 位数 m の2つの部分群は共役である．

（3） m の約数 m' を位数とする部分群は位数 m のある部分群に含まれる．

（4） 位数 m の部分数の個数 h_m は次の性質を満たす因子の積で表わされる；各因子は，（a）m を割るある素数を法として1と合同であり，（b）素数巾であって G の主組成因子の一つの約数である．

証：m が素数巾 p^a であれば（1），（3）は Sylow の第一定理（定理 4.2.1）であり（2）は Sylow の第二定理，（4）は Sylow の第三定理より強い主張で述べられたものである．

証明は G の位数に関する帰納法で示す．G の位数が素数巾ならこの定理の成立は明らかである．証明は定理 8.3.3 で与えられた G の主組成列の構造と商群の構造を主としてもとにする（定理 2.3.4）．

Case 1. G が位数 m_1n_1，指数 m_2n_2 の真正規部分群 H を含み $m=m_1m_2$，$n=n_1n_2$，$n_1<n$ が成立する．

（1） 帰納法の仮定から G/H は位数 m_2 の部分群を含みそれに対応する G の部分群 D の位数は mn_1 である．再び帰納法の仮定から D は位数 m の部分群を含む．

（2） M, M' を位数 m の二つの部分群とすると $M\cup H/H\cong M/M\cap H$（定理 2.4.1）が成り立つから $M\cup H=MH$，$M'\cup H=M'H$ は $m_1m_2\cdot m_1n_1$ の約数を位数にもつ部分群である．その位数は mn の約数でもあるから mn_1 の

約数でなければならない．一方位数は m, n_1 の倍数でもあるから $M \cup H$, $M' \cup H$ の位数は共に $mn_1 = m_1 n_1 m_2$ となり $M \cup H/H$, $M' \cup H/H$ は G/H の位数 m_2 の部分群となる．したがって帰納法の仮定からこれらは共役である．もし G/H の元 a^* により $M' \cup H/H$ が $M \cup H/H$ に変換され，Gの元aが準同型 $G \to G/H$ により a^* に写されるとすればこの準同型写像により $a^{-1}(M' \cup H)a$ は $M \cup H/H$ に写される．換言すれば $a^{-1}(M' \cup H)a = M \cup H$ が成り立つ．$a^{-1}M'a$, M は $M \cup H$ の位数mの部分群であるから帰納法の仮定により共役である．したがって M, M' はGで共役となる．

（3） M_1 を m の約数 m' を位数とする部分群とすると $M_1 \cup H/H$ の位数は m_2 の約数であるから G/H の位数 m_2 のある部分群に含まれる．したがって M_1 はそれに対応するGの位数 $m \cdot n_1$ の部分群に含まれるから帰納法の仮定から M_1 は位数mのある部分群に含まれる．

（4） （2）の証明から位数mの部分群Mと共役な部分群の個数 h_m は，G/H の位数 m_2 の部分群の個数 h_{m_2} と $M \cup H = D$ におけるMと共役な部分群の個数との積である．ここにDの主組成因子はGの主組成因子を割り切り，G/H の主組成因子はGの主組成因子の部分集合であるから帰納法の仮定から h_m は（4）を満たす二つの因子の積として表わされる．

さて主組成列における最小正規部分群の位数はpを素数として p^a とかける．もし $n = p^a$ でないとするとKは Case 1 のHに対する要求を満たすことになる．したがってすべての極小正規部分群は位数が p^a であると仮定してよい．ただし位数 p^a の Sylow 部分群としてはただ一つしか存在し得ない．

Case 2. Gが位数 $n = p^a$ の極小正規部分群Kをただ一つ持つ．

（1） Kを真部分群として含む極小正規部分群をLとすると L/K はqをpと異なる素数として q^b の位数を持つ．Qを位数 q^b のLの Sylow 部分群，MをG中Qの正規化群とし $M \cap K = T$ と置く．TはMの正規部分群であり，かつKの部分群でもあるから基本可換群である．Tの元とQの元の交換子は $T \cap Q = 1$ に含まれるからTの各元とQの各元は可換である．したがってTは

Lの中心Cに含まれ，CはLの特性部分群であるからGの正規部分群である．Kは唯一の極小正規部分群であるから $C=K$ か $C=1$ が成り立つ．もし $C=K$ とすると $L=K\times Q$ からQがGの正規部分群となりKの一意性に反する．したがって $T=C=1$ となりL中Qの正規化群はQであるからL中でのQの共役部分群の個数はQのLに対する指数に等しい．すなわちQはL中 $n=p^a$ 個の共役部分群を持つ．このときMのGに対する指数は $n=p^a$ となり位数はmとなる．

（2）と（4）　p^a 個のQの共役部分群の正規化群は互いに共役かつ相異なるから位数mの共役部分群が p^a 個得られる．またLにおける位数 q^b の部分群の個数から $p^a\equiv 1\ (\mathrm{mod.}\ q)$ が成り立つ．さてM'を位数mの任意の部分群とすると $M'\cup L$ の位数は m, n のいずれによっても割り切れるから $M'\cup L=G$ となる．$G/L\cong M'/M'\cap L$ から $M'\cap L$ の位数は q^b となりQと共役である．また$M'\cap L$ は M' 中正規ゆえ M' はQのある共役部分群の正規化群である．したがってすでに得られた p^a 個の位数mの共役部分群で位数mの部分群は尽きている．これで（2）と（4）が示された．

（3）　M'を位数 m' の部分群とする．ただし $m'|m$ とする．このときもしMの位数がmであれば $M\cap(M'\cup K)=M^*$ の位数は m' であって $M'\cup K$ に対する条件（2）からM'と共役である．したがってM'はMの共役部分群に含まれることになる．

可解群についての上述の性質は単純群においては一般には成立しない．位数60の単純群（5次の交代群）は位数15の部分群を持たないから（1）は成立しない．また (123) と (12)(45) で生成される位数6の部分群を含む位数12の部分群は存在しないから（3）は成立しない．最後に位数5の Sylow 群の個数は6で $6=2\cdot 3$ であるから（4）も成立しない．位数8の基本可換群Aの自己同型群は位数168の単純群Gである．GはAの7個の位数2の部分群の上に可移的に働き，また7個の位数4の部分群の上にも可移的に働く．したがってGは指数が7すなわち位数24の共役でない二つの部分群を持つことになり（2）に反する．

定理 9.3.1 の（1）は，可解群を特徴づける．このことを示すには第16章で定理 16.8.7 として証明される次の定理が必要である．

定理 9.3.2. (**Burnside**) 位数 $p^a q^b$ の群は可解群である．ただし p, q は素数である．

この定理を仮定すれば（1）でもって可解群を特徴づけることができる．位数 g の群 G において p 補群とは g を割る p の最高巾 p^e を指数にもつ部分群 S'_p のことである．しからば（1）は可解群においては p 補群が存在することを示し，Burnside の定理を使えばその逆が証明される．

定理 9.3.3. 群 G が位数を割るすべての素数 p に対し p 補群を含めば G は可解群である．

証：G の位数 g を $g=p_1^{e_1}\cdots p_r^{e_r}$ と素因数分解する．H_1, H_2 をそれぞれ $p_i^{e_i}, p_j^{e_j}$ の指数を持つ部分群とすれば指数が互いに素であるから（定理 1.5.6）$H_{12}=H_1\cap H_2$ の指数は $p_i^{e_i}p_j^{e_j}$ である．H_{12} と p_k 補群との共通部分は再び定理 1.5.6 により指数 $p_i^{e_i}p_j^{e_j}p_k^{e_k}$ の部分群である．この操作を続けていけば $(m, n)=1$ に対し $g=mn$ と分解したとき位数 m 指数 n の部分群を見出すことができてその部分群は n を割る素数 p に対する p 補群の共通部分となっている．したがって指数 n と互いに素な位数 m の部分群の存在を示すことすなわち（1）を示すには p 補群の存在を示せばよい．

帰納法でこれを示すために g より小さい位数の群に対しては定理が成立していると仮定する．位数 p^a の群においては任意の極大部分群は指数 p を持ち，かつ正規部分群であるから（系 4.1.2）位数 p^a の群は可解群である．Burnside の定理 9.3.2 を仮定すれば G の位数が少なくとも三つの異なる素数で割り切れる場合のみを考えればよい．p, q を g を割る異なる素数としたとき G は位数 $m=p^a q^b$ が指数 n と互いに素なる部分群 H を含む．H は可解群であるから素数巾の位数を持つ基本可換群 K を極小正規部分群として含む（定理 9.2.4）．その位数を p^i とする．さて K は位数 p^a の Sylow 部分群 $P\subseteq H\subseteq G$ に含まれている．G 中の q 補群 L^* は G 中 P と共役な Sylow 部分群 P^* を含むから

Gのある元の変換によってL^*はPを含むq補群Lに写される．ここに $L\supseteq P$, $H\supseteq P$ であるから位数を考えることにより $G=L\cup H$, $L\cap H=P$ が得られ LH は異なるg個の元を含むから $G=LH$ となる．したがってLによるGの各剰余類はHの元を含むからLのすべての共役部分群はHの元hによる変換によって得られる．一方KはH中正規ゆえ $h^{-1}Kh=K$ から $h^{-1}Lh\supseteq K$ が成立する．したがってLと共役な部分群全体の共通部分Mは $K\subseteq M\subset L$ からGの真部分群でありかつG中正規である．

よってGは真正規部分群Mを含む．もし S'_p をGのp補群とすれば $S'_p\cap M$ はMのp補群であり $S'_p\cup M/M$ は G/M のp補群であるから $M, G/M$ はともにp補群を持つことになり帰納法により可解群となる．ゆえにGは可解群である．

9.4. 可解群に関する2，3の結果

定理 9.4.1. Gを位数gの可解群，nをgの約数で $x^n=1$ が丁度n個の解を持つような数とすれば，それらの解全体はGの正規部分群をなす．

証：gが素数のとき定理の成立は明らかであるからgより小さい位数の可解群に対してこの定理が成立していると仮定する．Gは可解群ゆえ位数 p^i の基本可換群Kを極小正規部分群に持つ．ここでpがnを割る場合と割らない場合に分けて考える．

Case 1. pがnを割り切る．

Kの各元の位数は（単位元以外）pであるから $x^n=1$ の解である．ここで $n=p^in_1$, $g=p^sg_1$ と置くと G/K の位数は $p^{s-i}g_1$ であるから $j\geqq i$ のときは $u=p^{j-i}n_1$ で，また $j<i$ のときは $u=n_1$ でそれぞれ割り切れる．したがって G/K には $z^u=1$ なる元zが ku 個ある．さてxをGの元で準同型 $G\to G/K$ で $x\to z$, $z^u=1$ なるものとすると $x^u\in K$ であるから $x^{up}=1$ が成立し up はnの約数であるからそのような元xに対し $x^n=1$ が成り立つ．しかるにこのようなxは G/K 中Kの ku 個の剰余類の元であるから少なくとも kup^i 個

の $x^n=1$ を満たすGの元が存在する．もし $j<i$ とすると up^i はnの真の倍数であるから $x^n=1$ がnより多くの解を持つことになり仮定に反する．したがって $j\geqq i$ であって $up^i=n$ から少なくとも kn 個の解を持つことになり $k=1$ が得られて G/K の中に $z^u=1$ の解が丁度u個存在することになる．帰納法の仮定によりこれらu個の解は G/K の正規部分群 H/K をなしGにおいてこの群に対応する部分群Hは位数 $up^i=n$ の正規部分群であってその元は $x^n=1$ のn個の解となっている．

Case 2. pがnを割らない．

nは G/K の位数の約数であるから G/K には $z^n=1$ の解は kn 個ある．もし自然な準同型によりGの元yが $y\to z$ であったとすれば $y^n\in K$ から $y^{pn}=1$ が成立する．したがってGには $y^{pn}=1$ を満たす元yを含むKによる剰余類が kn 個ある．各剰余類 Ky から異なる $x^n=1$ の解が得られることを示そう．Ky_1, Ky_2 をKの異なる剰余類とし $y_1\to z_1$, $y_2\to z_2$, $z_1\neq z_2$ であったとすると $y_1{}^{pn}=1$, $y_2{}^{pn}=1$ であるから $y_1{}^p=x_1$, $y_2{}^p=x_2$ は $x^n=1$ のGにおける解である．もし $y_1{}^p=y_2{}^p$ とすると $z_1{}^p=z_2{}^p$ が成立するが $z_1{}^n=1$, $z_2{}^n=1$, かつ $(p,n)=1$ であるから $z_1=z_2$ となり仮定に反する．したがって $z^n=1$ が G/K に kn 個の解を持てば $x^n=1$ はGに少なくとも kn 個の解を持つことになるから $k=1$ でなければならない．ゆえに帰納法の仮定から G/K は位数nの正規部分群 U/K を含む．Gにおいて U/K に対応する群Uの位数は p^in である．Uは可解群であるから位数nのp補群Hを含む．Hのn個の元は $x^n=1$ の解でありGの任意の元によりHの元を変換して得られた元も $x^n=1$ の解となるからHはGの正規部分群である．

定理 9.4.2. 群Gの交換子群鎖 $G'\supset G''\supset G'''\supset\cdots$ において連続した二つの商群がともに巡回群ならば後の商群は単位群である．

証：G'/G'', G''/G''' を巡回群とし $G'''=1$ としたとき $G''=1$ なることを示せばよい．G'' の生成元をbとする．GはG''の正規化群であるからZ_bをG''の中心化群とすると G/Z_b は巡回群の自己同型群の部分群に同型であるから可

換群である．したがって $Z_b \supseteq G'$ が成立し G'' は G' の中心に含まれ，かつ G' は G'' と一つの元から生成されている．よって G' は可換群となり $G''=1$ が成り立つ．

G/G', G' がともに巡回群なるとき G を**メタ・サイクリック群**という．このとき $G''=1$ であるから長さが2のメタ・サイクリック群が存在する．定理 9.4.2 により長さ3のメタ・サイクリック群は存在しない．

定理 9.4.3. 位数 g の有限群 G の Sylow 部分群がすべて巡回群であれば G はメタ・サイクリック群であって次の関係を持つ二元 a, b で生成される：

$$a^m=1,\quad b^n=1,\quad b^{-1}ab=a^r,$$
$$mn=g,$$
$$[(r-1)n, m]=1,$$
$$r^n\equiv 1 \pmod{m}.$$

逆にこのような関係を持つ二元で生成された群の Sylow 部分群はすべて巡回群である．

証：まず G が可解群なることを示そう．$g=p_1^{e_1}\cdots p_s^{e_s}$, $p_1<p_2<\cdots<p_s$, を g の素因子分解とし $m=p_j^{f_j}p_{j+1}^{e_{j+1}}\cdots p_s^{e_s}$, $f_j\leqq e_j$, に対し $x^m=1$ が丁度 m 個の解を持つことを示す．$m=g$ のときは明らかであるから $x^{mp}=1$ が丁度 mp 個の解を持ち p が mp を割る最小の素数であれば $x^m=1$ が丁度 m 個の解を持つことを示せば十分である．p-Sylow 部分群は巡回群であるから p^{f+1} を pm を割る p の最高巾とすれば G には位数 p^{f+1} の元があるから $x^{mp}=1$ の解がすべて $x^m=1$ の解となることはない．したがって $x^m=1$ の km 個の解（定理 9.1.2）は $x^{mp}=1$ の解全体を与えていないから $1\leqq k<p$ が成立する．$x^{mp}=1$ を満たすが $x^m=1$ は満たさない元の位数 t は p^{f+1} できっかり割れる．位数がきっかり p^{f+1} で割れ，かつ同じ巡回群を生成する元が $\varphi(t)$ 個ある．p^{f+1} が t の約数であるから $\varphi(t)$ は $p-1$ で割れる．したがって $x^{mp}=1$ を満たし $x^m=1$ を満たさない元の数 $pm-km=(p-k)m$ は $p-1$ で割り切れる．p は mp を割る最小の素数であったから $p-1$ と m とは互いに素である．したがっ

て $p-1$ は $p-k$ の約数であり $1\leqq k<p$ から $k=1$ が得られる．すなわち $x^m=1$ が丁度m個の解を持つ．特に $m=p_s^{e_s}$ のときも $x^m=1$ は丁度m個の解を持つが位数mの Sylow 部分群が存在するからこの Sylow 部分群はGの正規部分群でなければならずかつ巡回群であるからもちろん可解群である．

Sylow 部分群がすべて巡回群である群Gは正規部分群Hを持つことが分ったが $H, G/H$ の Sylow 部分群も巡回群であるから素数位数の群が可解群なることから帰納的に $H, G/H$ がともに可解群と仮定することによりGが可解群となる．

Sylow 部分群がすべて巡回群なる可換群は巡回群であるから列 $G\supset G'\supset G''\supset\cdots$ において商群はすべて巡回群である．したがって定理 9.4.2 により $G''=1$ が成り立つ．もし $G'=1$ とするとGは巡回群であってこのとき $b=1$, $r=1$, $n=1$, $m=g$ とすればよいから $G'\neq 1$ と仮定してよい．G' の生成元を a とし $a^m=1$ とする．またbを巡回群 G/G' の生成元である剰余類 $G'b$ の元とする．しからば a, b はGを生成し G' がGで正規なることから $b^{-1}ab=a^r$ が成立し $r\neq 1$ である．なぜならば $r=1$ のときはGは可換群となり $G'\neq 1$ に反するからである．いま G/G' の位数をnとすると $b^{-n}ab^n=a^{r^n}=a$ となり $r^n\equiv 1$ (mod. m) が成り立つ．さてGの各元は b^ja^i の形をしているから一般の交換子 (b^ua^v, b^ja^i) は (a^k, b^t) なる形の元の交換子として表わされる．一方 (a^k, b^t) は $a^{-1}b^{-1}ab=a^{r-1}$ の巾で表わされる．したがって a^{r-1} は G' を生成することになり $(r-1, m)=1$ が成り立つ．さて b^n は G' の元であるからaの巾 a^j に等しくかつbと可換であるから $a^{rj}=a^j$ が成立するが $(r-1, m)=1$ であるから $j=0$ であって $b^n=1$ となる．もしmとnがともに素数pで割り切れるとすれば $a^{m/p}$ と $b^{n/p}$ は位数 p^2 の非巡回群を生成することになり仮定に反する．したがって $(m, n)=1$ が得られて定理の前半が示されたことになる．

逆に m, n, r, g が定理の関係を満たすとすれば $r^n\equiv 1$ (mod. m) であるから $a\to a^r$ はaで生成される巡回群の自己同型であってそのn乗は単位元である（n乗より小さい巾で単位元になることもある）．したがって mn 個の元

$b^j a^i$, j mod. n, i mod. m, の乗法則 $b^j a^i \cdot b^k a^t = b^{j+k} \cdot a^h$, $h = ir^k + t$, に関し結合律と逆元の存在が示されて $a^m = 1$, $b^n = 1$, $b^{-1}ab = a^r$ なる関係を持つ位数 $g = mn$ の群が得られる．この群において各交換子は $a^{-1}b^{-1}ab = a^{r-1}$ の巾であり $(r-1, m) = 1$ であるから G' は a で生成される．また $(m, n) = 1$ から各 Sylow 部分群は部分群 $\{a\}$ か $\{b\}$ の共役部分群に含まれるから巡回群である．

系 9.4.1. 平方因子を持たない位数の群は定理 9.4.3 に述べられた型のメタ・サイクリック群である．

これは Sylow 部分群がすべて素数位数したがって巡回群なることから明らかである．

演 習 問 題

1. 有限群 G の位数が 12 の倍数で $x^{12} = 1$ の解が G の中に丁度 12 個あるとすれば，それらの解全体は G の正規部分群をなすことを示せ．
2. p, q を異なる素数とし群 G が p^2q なる位数を持つとすれば Sylow 部分群の中に G の正規部分群が存在し，したがって G が可解群となることを示せ．
3. p, q, r を異なる素数とし群 G が p^2qr の位数を持つとする．このとき G は可解群であるか位数 60 の 5 次の交代群（に同型）であることを示せ．（定理 14.3.1 とその系を使え）
4. $x^n = 1$ の解が G の中に丁後 m 個あってそれらを $x_1 = 1, x_2, \cdots, x_m$ とする．このとき $K = \{x_1, \cdots, x_m\}$ は G の正規部分群であって K の元は $x_2^{a_2} x_3^{a_3} \cdots x_m^{a_m}$ の型でありしかも K の位数は n^{m-1} 以下となることを示せ．

第10章　超可解群と巾零群

10.1. 定　　　義

群において可解性より強い性質であってしかもかなり重要なものが二つある．それらは超可解性と巾零性である．

定　義：群 G が有限不変列 $G=A_0\supseteq A_1\supseteq A_2\supseteq\cdots\supseteq A_r=1$ を持ち各商群 A_{i-1}/A_i が巡回群のとき G を超可解群という．

定　義：群 G が有限不変列 $G=A_0\supseteq A_1\supseteq A_2\supseteq\cdots\supseteq A_r=1$ を持ち $i=1,\cdots,r$ に対し A_{i-1}/A_i が G/A_i の中心に含まれるとき G を**巾零群** (nilpotent group) という．

どちらの場合も A_{i-1}/A_i は可換群であるからこれらの性質は G が可解群なることを示している．超可解群 G においては巡回群 A_{i-1}/A_i の生成元に（自然な準同型により）写される A_{i-1} の任意の元 b_{i-1} に対して $A_{i-1}=\{b_{i-1}, A_i\}$ が成立するから G は有限生成である．すべての可換群は巾零群であるから巾零群が必らずしも有限生成でないことは明らかである．

Baer [12] はより一般な形で超可解性を定義している．すなわち G の各準同型像が巡回正規部分群を含むとき G を超可解群と定義した．彼は有限生成の群に対してはこの定義と我々の定義とが同値なることを示しているが，この章で示される性質は広い意味での定義では成立しない．

10.2. 降中心列と昇中心列

交換子 $x^{-1}y^{-1}xy$ を (x, y) とかく．また部分群 A, B に対し $a\in A,\ b\in B$ なる元 a, b の交換子 (a, b) 全体で生成された群を (A, B) で表わす．

$$(x_1, \cdots, x_{n-1}, x_n) = ((x_1, \cdots, x_{n-1}), x_n)$$

により**単純交換子**を定義した．そこで部分群 $A_1, \cdots, A_{n-1}, A_n$ に対しても同様に

$$(A_1, \cdots, A_{n-1}, A_n) = ((A_1, \cdots, A_{n-1}), A_n)$$

と定義する．また共役は巾指数で表わす．すなわち

$$a^x = x^{-1}ax$$

とかく．このとき高位の交換子に関する一連の重要な等式が成立する：

(10.2.1.1)　$(y, x) = (x, y)^{-1}$,

(10.2.1.2)　$(xy, z) = (x, z)^y(y, z) = (x, z)(x, z, y)(y, z)$,

(10.2.1.3)　$(x, yz) = (x, z)(x, y)^z = (x, z)(x, y)(x, y, z)$,

(10.2.1.4)　$(x, y^{-1}, z)^y(y, z^{-1}, x)^z(z, x^{-1}, y)^x = 1$,

(10.2.1.5)　$(x, y, z)(y, z, x)(z, x, y)$

$$= (y, x)(z, x)(z, y)^x(x, y)(x, z)^y(y, z)^x(x, z)(z, x)^y.$$

これらの等式は交換子の定義から直接計算により導かれる．

次の法則により群 G の部分群の列を定義する．G の任意の元 x_i に対し

$$\Gamma_1(G) = G,$$
$$\Gamma_k(G) = \{(x_1, \cdots, x_k)\}$$

と置く．

$(y_1, y_2, \cdots, y_{k+1}) = [(y_1, y_2), y_3, \cdots, y_{k+1}]$ であるからすべての k に対して $\Gamma_{k+1}(G) \subseteq \Gamma_k(G)$ が成立する．明らかに $\Gamma_k(G)$ は G の全不変部分群である．

$$G = \Gamma_1(G) \supseteq \Gamma_2(G) \supseteq \cdots$$

なる G の鎖を G の**降中心鎖** (lower central series) という．

定理 10.2.1. $\Gamma_{k+1}(G) = (\Gamma_k(G), G)$.

証：$(y_1, \cdots, y_k, y_{k+1}) = ((y_1, \cdots, y_k), y_{k+1})$ から $\Gamma_{k+1}(G) \subseteq (\Gamma_k(G), G)$ が成立している．逆の包含関係を示すために等式 (10.2.1.1), …, (10.2.1.5) を使う．(10.2.1.2) において $x = (a_1, \cdots, a_k)$, $y = (a_1, \cdots, a_k)^{-1}$, $z = a_{k+1}$ と置くと $1 = (1, a_{k+1}) = (a_1, \cdots, a_k, a_{k+1})^y((a_1, \cdots, a_k)^{-1}, a_{k+1})$ が成立するから $((a_1, \cdots,$

$a_k)^{-1}, a_{k+1})\in\Gamma_{k+1}(G)$ が得られる．さて $(\Gamma_k(G), G)$ は，u_i を $u_i=(a_1, \cdots, a_k)$ か $u_i=(a_1, \cdots, a_k)^{-1}$ と置くとき $(u_1u_2\cdots u_n, g)$ なる元で生成される．$(u_i, g)\in \Gamma_{k+1}(G)$ なることはすでに示されているので n に関する帰納法によって $(u_1u_2 \cdots u_n, g)\in\Gamma_{k+1}(G)$ を示そう．そのため (10.2.1.2) において $x=u_1u_2\cdots u_{n-1}$, $y=u_n$, $z=g$ と置くと $(u_1\cdots u_{n-1}u_n, g)=(u_1\cdots u_{n-1}, g)^{u_n}(u_n, g)$ が成立し帰納法の仮定により右辺の二元はともに $\Gamma_{k+1}(G)$ に含まれる．したがって $(\Gamma_k(G), G)\subseteq\Gamma_{k+1}(G)$ が成立することになり定理が示された．

この定理から重要な次の系が導びかれる．

系 10.2.1. $\Gamma_k(G)/\Gamma_{k+1}(G)$ は $G/\Gamma_{k+1}(G)$ の中心に含まれる．

任意の群 G に対し**昇中心鎖** (upper central series) を次のように定義する．

$$Z_0=1\subseteq Z_1(G)\subseteq Z_2(G)\subseteq\cdots\subseteq Z_i(G)\subseteq Z_{i+1}(G)\subseteq\cdots$$

なる鎖において $Z_{i+1}(G)/Z_i(G)$ が $G/Z_i(G)$ の中心であるときこの鎖を**昇中心鎖**という．群の中心は特性部分群であるから（しかし一般には全不変部分群ではない）各 Z_i は G の特性部分群である．次の定理は定義した中心鎖につけられた**昇**と**降**の意味を正当化するものである．

列 $G=A_1\supseteq A_2\supseteq A_3\supseteq\cdots\supseteq A_{r+1}=1$ において各 A_i/A_{i+1} が G/A_{i+1} の中心に含まれるときこの列を**中心列** (central series) という．

定理 10.2.2. $G=A_1\supseteq A_2\supseteq A_3\supseteq\cdots\supseteq A_{r+1}=1$ を G の中心列とすれば $i=1, \cdots, r+1$ に対し $A_i\supseteq\Gamma_i(G)$ がまた $j=0, 1, \cdots, r$ に対し $A_{r+1-j}\subseteq Z_j(G)$ がそれぞれ成立する．

証：$A_1=G=\Gamma_1(G)$ である．$A_i\supseteq\Gamma_i(G)$ であると仮定しよう．A_i/A_{i+1} は G/A_{i+1} の中心に含まれるから $(A_i, G)\subseteq A_{i+1}$ が成立する．したがって $\Gamma_{i+1}(G)=(\Gamma_i(G), G)\subseteq(A_i, G)\subseteq A_{i+1}$ から帰納法によりすべての i に対し $A_i\supseteq\Gamma_i(G)$ が成立する．次にある i に対して $A_{r+1-i}\subseteq Z_i(G)$ であったとすると $T=G/Z_i(G)$ は $U=G/A_{r+1-i}$ の準同型像であってその核は $Z_i(G)/A_{r+1-i}$ である．さて A_{r-i}/A_{r+1-i} は U の中心に含まれているから T の中においてその準同型像は T の中心に含まれなければならない．しかるにこの準同型像は $A_{r-i}\cup$

Z_i/Z_i でありまたTの中心は Z_{i+1}/Z_i であるから $A_{r-i}\subseteq A_{r-i}\cup Z_i\subseteq Z_{i+1}$ が成立し帰納法により定理の後半も示されたことになる．

この定理の帰結として次の系が得られる．

系 10.2.2. 巾零群Gにおいては昇中心鎖および降中心鎖は有限の長さを持ちかつともに同じ長さcとなる．

もし長さrの中心列があれば定理により昇中心列および降中心列の長さはたかだかrであり二つの列を比べることによりともに等しい長さcを持つことが分かる．このcを巾零群の**級**（class）という．級1の巾零群は可換群である．

定理 10.2.3. 群Gが元 $x_1, \cdots, x_r$ で生成されるならば $\Gamma_k(G)/\Gamma_{k+1}(G)$ は単純交換子 $(y_1, y_2, \cdots, y_k)$ mod. $\Gamma_{k+1}(G)$ で生成される．ここに $y_1, \cdots, y_k$ は $x_1, \cdots, x_r$ のどれかであって必ずしも異ならなくてもよい．

系 10.2.3. もしGがr個の元で生成されるなら $\Gamma_k(G)/\Gamma_{k+1}(G)$ はたかだか r^k 個の元で生成される．

証：$k=1$ のとき定理が成立することは明らかであるからkに関する帰納法で証明する．$k-1$ のとき定理が成立していると仮定する．$\Gamma_k(G)$ は $a_i\in G$ なる a_i に対し $C=(a_1, \cdots, a_{k-1}, a_k)$ なる交換子全体で生成されているが $C=((a_1, \cdots, a_{k-1}), a_k)$ において $(a_1, \cdots, a_{k-1})\in\Gamma_{k-1}(G)$ であるから帰納法の仮定により y_i を $x_1, \cdots, x_r$ のどれかとし $u_1, \cdots, u_n$ を $(y_1, \cdots, y_{k-1})$ なる形の交換子としまた $w\in\Gamma_k(G)$, $\epsilon_i=\pm1$ としたとき $(a_1, \cdots, a_{k-1})=u_1^{\epsilon_1}u_2^{\epsilon_2}\cdots u_n^{\epsilon_n}w$ が成立する．したがって $C=(u_1^{\epsilon_1}u_2^{\epsilon_2}\cdots u_n^{\epsilon_n}w, a_k)$ となるが (10.2.1.2) を使うと $C=(u_1^{\epsilon_1}u_2^{\epsilon_2}\cdots u_n^{\epsilon_n}, a_k)(u_1^{\epsilon_1}u_2^{\epsilon_2}\cdots u_n^{\epsilon_n}, a_k, w)(w, a_k)\equiv(u_1^{\epsilon_1}u_2^{\epsilon_2}\cdots u_n^{\epsilon_n}, a_k)$(mod. Γ_{k+1}) が成立する．さて $a_k=x_{i_1}^{\eta_1}\cdots x_{i_m}^{\eta_m}$, $\eta_j=\pm1$ であり各iに対して $u_i\in\Gamma_{k-1}$ から (10.2.1.2), (10.2.1.3) を繰り返し使うことにより mod. Γ_{k+1} でCは交換子 $(u_j^{\epsilon_j}, x_{i_s}^{\eta_s})$ の積として表わされることが分る．しかるに $(u^{\epsilon}, x^{\eta})\equiv(u, x)^{\epsilon\eta}$ (mod. $\Gamma_{k+1}(G)$) が成り立つから $\Gamma_k(G)/\Gamma_{k+1}(G)$ は交換子 (u, x) mod. $\Gamma_{k+1}(G)$ か交換子 $(y_1, \cdots, y_{k-1}, x_{i_k})$ mod. $\Gamma_{k+1}(G)$ で生成されること

になる．これが証明すべきことであった．この定理で r の有限性は必要でないことに注意せよ．

この定理の直接の帰結として次の定理すなわち巾零群と超可解群との間の関係が得られる．

定理 10.2.4. 有限生成の巾零群は超可解群である．

証：G を有限生成の巾零群としその降中心列を

$$G=\Gamma_1(G)\supset\Gamma_2(G)\supset\cdots\supset\Gamma_c(G)\supset\Gamma_{c+1}(G)=1$$

とする．$\Gamma_c(G)$ は可換群かつ有限生成であるから m 個の巡回群の直積として表わされる．また $\Gamma_c(G)$ は G の中心に含まれるから $\Gamma_c(G)$ の任意の部分群は G の正規部分群である．したがって列 $\Gamma_{c+1}=1\subset\{a_1\}\subset\{a_1, a_2\}\subset\cdots\subset\{a_1, \cdots, a_m\}=\Gamma_c(G)$ に現われる部分群はすべて G で正規であり直後の群による商群がすべて巡回群である．同様に $\Gamma_{i+1}(G)$ と $\Gamma_i(G)$ の間に正規部分群を挿入し直後の群による商群がすべて巡回群となるようにできる．このようにして G の超可解性を定義する列を作ることができる．

系 10.2.4. 有限生成の巾零群は極大条件を満たす．

群 G の部分群の無限昇鎖が存在しないとき G は極大条件を満たすと定義したが，それは G の任意の部分群が有限生成なることと同値であった．定理 10.5.1 で超可解群の任意の部分群が超可解群なることを，したがって有限生成なることを示す．可解群においてはこれは正しくない．もし F を二元 a, b で生成される自由群とすれば F/F'' は可解群であるが F'/F'' は無限に多くの生成元 $a^{-i}b^{-j}a^ib^j$ を持つ．

10.3. 巾零群に関する定理

G が級 c の巾零群なら交換子 $(a_1, \cdots, a_{c+1})$ はすべて単位元であり，逆に $(a_1, \cdots, a_{c+1})=1$ が常に成立していれば G はたかだか級 c の巾零群である．すべての G の元 a_i に対し $(a_1, \cdots, a_{c+1})=1$ が成り立つとき G は nil-c を持つと

いう.

定理 10.3.1. Gが nil-c を持てばGの任意の部分群および商群も nil-c を持つ.

証：Gが nil-c を持てば部分群Hに対して $a_i \in H$ のときすべての交換子 $(a_1, \cdots, a_{c+1})$ は1に等しいからHも nil-c を持つ. またTをGの準同型像とすると b_i をTの元としたとき任意の交換子 $(b_1, \cdots, b_{c+1})$ はGにおけるある交換子 $(a_1, \cdots, a_{c+1})$ の準同型像になっているから単位元となる. したがってTは nil-c を持つ.

次の定理は巾零群とは限らない群Gの巾零正規部分群に適用される.

定理 10.3.2. H, K をGの正規部分群としHが nil-c を, またKが nil-d をそれぞれ持てば $H \cup K = HK$ は nil-$(c+d)$ を持つ.

証：$h_i \in H,\ k_i \in K$ に対し $u_i = h_i k_i$ と置くと $\Gamma_m(HK)$ は $(u_1, u_2, \cdots, u_m)$ なる交換子すべてで生成される. 各 v_i をHかKの元としたとき $(u_1, u_2, \cdots, u_m)$ が $w = (v_1, v_2, \cdots, v_m)$ なる形の交換子の積として表わされることを示そう. $m=1$ のときこのことは明らかである. $m-1$ のとき成立すると仮定すれば (10.2.1.3) と H, K がGの正規部分群なることを使って次の等式をうる.

$$\begin{aligned}(u_1, \cdots, u_{m-1}, u_m) &= (w_1 w_2 \cdots w_t, h_m k_m)\\ &= (w_1 \cdots w_t, k_m)(w_1 \cdots w_t, h_m)^{k_m}\\ &= (w_1 \cdots w_t, k_m)(w_1{}^{k_m} \cdots w_t{}^{k_m}, h_m{}^{k_m})\\ &= (w_1 \cdots w_t, k_m)(w_1' \cdots w_t', h_m').\end{aligned}$$

同様にして (10.2.1.2) を使うことにより

$$\begin{aligned}(w_1 \cdots w_t, k_m) &= (w_1, k_m)^{w_2 \cdots w_t}(w_2 \cdots w_t, k_m)\\ &= (w_1'', k_m'')(w_2 \cdots w_t, k_m)\end{aligned}$$

が成立する. この操作を続けていけば最後には $(u_1, \cdots, u_{m-1}, u_m)$ は $(w, h_m{}^{(i)})$ と $(w, k_m{}^{(i)})$ との積として表わされることになる. ここに $(w, h_m{}^{(i)}), (w, k_m{}^{(j)})$ は各 v_i がHかKの元を表わすとき $(v_1, \cdots, v_m)$ という形をしている. ゆえに帰

納法により我々の主張の正しいことが示された．$\Gamma_{c+d+1}(HK)$ が各 v_i を h か $k, h\in H$, $k\in K$, としたとき交換子 $(v_1, \cdots, v_{c+d+1})$ で生成されることはすでにみた．また一般に $(v_1, \cdots, v_{t-1}, v_t)=(v_1, \cdots, v_{t-1})^{-1}v_t^{-1}(v_1, \cdots, v_{t-1})\ v_t$ が成立している．HK において $\Gamma_i(H)$ は正規であるから $(v_1, \cdots, v_{t-1})\in\Gamma_i(H)$ であるとすれば v_t が k のときは $(v_1, \cdots, v_t)\in\Gamma_i(H)$ が，また v_t が h のときは $(v_1, \cdots, v_t)\in\Gamma_{i+1}(H)$ がそれぞれ成立する．したがって $(v_1, \cdots, v_{c+d+1})$ において $(c+1)$ 個の h があればこの交換子は $\Gamma_{c+1}=1$ に含まれるから単位元となる．もし $(c+1)$ 個の h がないときは少なくとも $(d+1)$ 個の k が $(v_1, \cdots, v_{c+d+1})$ の中にあるからこの交換子は $\Gamma_{d+1}=1$ に含まれることになる．いずれの場合も $(v_1, \cdots, v_{c+d+1})=1$ が成立するから $H\cup K=HK$ は nil-$(c+d)$ を持つ．

定理 10.3.3. 群 G が nil-c を持ち $H=H_0$ を G の任意の部分群，H_{i+1} を H_i の G における正規化群とすると $H_c=G$ となる．

証：$H_0\supseteq Z_0=1$ は明らかに成立する．帰納法によりすべての m に対し $H_m\supseteq Z_m$ が成立することを示そう．さて $H_i\supseteq Z_i$ と仮定すると Z_{i+1} の定義から任意の Z_{i+1} の元 z_{i+1} と任意の G の元 g とに対し $z_{i+1}^{-1}g^{-1}z_{i+1}g=z_i\in Z_i$ が成立するから $g^{-1}=h_i\in H_i$ とすると $z_{i+1}^{-1}h_iz_{i+1}=z_ih_i\in H_i$ が成立し，したがって Z_{i+1} は H_i を正規化することになり $H_{i+1}\supseteq Z_{i+1}$ が成り立つ．よって帰納法により $H_m\supseteq Z_m$ がすべての m について成立することになる．しかるに $Z_c=G$ であるから $H_c=G$ が成り立つ．

系 10.3.1. 巾零群の任意の真部分群はその正規化群の真部分群である．

系 10.3.2. 巾零群の任意の極大部分群は素数指数を持つ正規部分群であって交換子群を含む．

M を巾零群 G の極大部分群とすると $N_G(M)$ は M を真部分群として含むから $N_G(M)=G$ がすなわち $M\lhd G$ が成り立つ．M の極大性により G/M は真部分群を含み得ないから素数位数の巡回群でなければならない．したがって

Mは素数指数を持ち G/M は可換となるから交換子群 G' はMに含まれる.

系 10.3.3. Gを巾零群, Hを $G=G'H$ を満たす部分群とすれば $H=G$ である.

もし $H\neq G$ とすると定理により $H=H_0$, $H_{i+1}=H_iZ_{i+1}$ に対して各 H_i は H_{i+1} の中で正規である. もし $H_j\neq G$ であって $H_{j+1}=G$ とすると H_j はGの真正規部分群であり G/H_j は可換群となるから $H_j\supseteq G'$ が成立する. しからば $HG'\subseteq H_jG'=H_j\neq G$ となって仮定に反する. したがって $H=G$ となる. ここではGが極大部分群を持つということは仮定しなかったことに注意しよう.

定理 10.3.4. 有限p群は巾零群である. 有限群が巾零群なるための必要十分条件はその群が Sylow 部分群の直積として表わされることである.

証:定理 4.3.1 により任意の有限p群Pは単位群と異なる中心を持っているからPの昇中心列はPに到達する. したがってPは巾零である. 同じ論法が有限p群の直積である群についても成立する. さてGを任意の有限巾零群, PをGの p-Sylow 部分群とすれば定理 4.2.4 によって $N_G(P)$ の正規化群は $N_G(P)$ であるから系 10.3.1 により $N_G(P)$ はGの真部分群ではあり得ない. したがって $P\lhd G$ である. Gの任意の Sylow 部分群が正規部分群であるからGは Sylow 部分群の直積である.

系 10.3.4. (**Wielandt**) 有限群が巾零群なることとその極大部分群が正規部分群なることとは同値である.

系 10.3.2 により巾零群の極大部分群は正規部分群である. 一方定理 4.2.4 によりPを p-Sylow 部分群とすると $N_G(P)$ はGの真正規部分群に含まれることはないから極大部分群が正規部分群であれば $P\lhd G$ が成立することになりGは Sylow 部分群の直積となる.

定理 10.3.5. X, Y, Z を群Gの部分群, Kを (Y, Z, X), (Z, X, Y) を含むGの正規部分群とすればKは (X, Y, Z) も含む.

証：(10.2.1.4) から

$$(x, y, z)=((z, x^{-1}, y^{-1})^{xy})^{-1}((y^{-1}, z^{-1}, x)^{zy})^{-1}$$

が得られて定理が成立する.

定理 10.3.6. $H=H_0\supseteq H_1\supseteq\cdots$ においてすべての H_i が群 G の正規部分群であり，ある部分群 L とすべての i に対し $(H_{i-1}, L)\subseteq H_i$ が成立するとすれば $(H_i, \Gamma_j(L))\subseteq H_{i+j}$ が成立する.

系 10.3.5. $(\Gamma_i(G), \Gamma_j(G))\subseteq\Gamma_{i+j}(G)$.

証：$j=1$ のときは仮定に含まれているから j に関する帰納法で証明をする. すべての i に対して $(H_i, \Gamma_{j-1}(L))\subseteq H_{i+j-1}$ が成立するとすれば帰納法の仮定により $(L, H_i, \Gamma_{j-1}(L))\subseteq(H_{i+1}, \Gamma_{j-1}(L))\subseteq H_{i+j}$ および $(H_i, \Gamma_{j-1}(L), L)\subseteq(H_{i+j-1}, L)\subseteq H_{i+j}$ が成り立つ. $(\Gamma_{j-1}(L), L)=\Gamma_j(L)$ であるから定理 10.3.5 が適用できて

$$(H_i, \Gamma_j(L))=(H_i, (\Gamma_{j-1}(L), L))=(\Gamma_{j-1}(L), L, H_i)\subseteq H_{i+j}$$

が成り立つから定理が証明されたことになる.

10.4. 群の Frattini 部分群

G を任意の群としたとき Frattini 部分群と呼ばれる G の部分群 Φ を次のように定義する：もし G が極大部分群を持つならば M を極大部分群すべてを動かしたとき $\Phi=G\bigcap_M M$ と定義する. したがって $\Phi=G$ と G が極大部分群を持たないこととは同値である. G の任意の自己同型は極大部分群を極大部分群に写すから Frattini 部分群は明らかに G の特性部分群である.

Frattini 部分群は G の生成系に関係を持つ群である. すなわち Frattini 部分群は次の定義の意味において G の非生成元全体からなる.

定　義：群 G の元 x は G の部分集合 T に対し $G=\{T, x\}$ ならば常に $G=\{T\}$ が成立するとき G の非生成元といわれる.

$\{T, x\}=G$ となる任意の集合 T に対し $\{T, x\}=\{T\}$ の成立を要求していることに注意しよう．$G\neq 1$ のとき 1 は非生成元である．

定理 10.4.1. 群 G が単位群でなければ Frattini 部分群 Φ は G の非生成元全体からなる．

証：G の元 x を含まない極大部分群 M があるとすれば群 $\{M, x\}$ は M を真部分群として含みかつ M が極大なることから $\{M, x\}=G$ となる．しかるに $\{M\}=M\neq G$ であるから x は $\{M, x\}=G$ の非生成元ではない．したがって G の非生成元はすべての極大部分群に含まれることになり $\Phi=G\bigcap_M M$ の元である．逆に $u\in\Phi$ のとき u が G の非生成元なることを示さねばならない．仮定により $G\neq 1$ であるから 1 は非生成元である．

さて G の部分集合 T に対し $G=\{T, u\}$ であったとし $\{T\}=H\neq G$ と仮定して矛盾を出そう．$H\neq G$ ならば $u\notin H$ である．なぜならばもし $u\in H$ とすると $H=\{H, u\}\supseteq\{T, u\}=G$ となるからである．したがって Zorn の補題により条件 $u\notin K$ に関して極大である部分群 $K\supseteq H$ が存在する．このとき $\{K, u\}\supseteq\{T, u\}=G$ であるから $\{K, u\}=G$ が成立する．一方 K の選びかたにより K を真に含む任意の部分群は u を含まねばならないから $K=M$ は u を含まない極大部分群となり $u\in\Phi=G\bigcap_M M$ に反する．したがって $\{T\}=G$ となり Φ の各元 u は G の非生成元である．

定理 10.4.2. 有限群の Frattini 部分群は巾零群である．

証：G を有限群，Φ を G の Frattini 部分群，P を Φ の p-Sylow 部分群とする．Φ は G の特性部分群であるから G の正規部分群である．したがって G の中での P の任意の共役部分群は Φ に含まれ Φ の p-Sylow 部分群となるから Φ の中で共役である．よって P は G の中でと同数の共役を Φ の中で持つことになり $[G:N_G(P)]=[\Phi:N_\Phi(P)]$ が成立する．しかるに $[G:N_\Phi(P)]=[G:\Phi][\Phi:N_\Phi(P)]=[G:N_G(P)][N_G(P):N_\Phi(P)]$ が成立しているから $[G:\Phi]=[N_G(P):N_\Phi(P)]$ が成立する．$N_\Phi(P)=N_G(P)\cap\Phi$ なるこ

とに注意して定理 1.5.5 の指数に関する不等式を使うと $[N_G(P)\cup\Phi:\Phi]\geq[N_G(P):N_G(P)\cap\Phi]=[G:\Phi]$ が得られて $N_G(P)\cup\Phi=G$ なることが結論される．さて $G=\{N_G(P),\Phi\}$ であるから Φ の元をすべて同時に取り去れば（これは Φ が有限群なることから可能である）$G=\{N_G(P)\}=N_G(P)$ が成立する．したがって $P\triangleleft G$ であるから $P\triangleleft\Phi$ でもある．Φ の任意の Sylow 部分群が正規部分群であるから Φ は Sylow 部分群の直積であって巾零群となる．

定理 10.4.3. 巾零群の Frattini 部分群は交換子群を含む．

証：Gが巾零群で $G=HG'$ であれば系 10.3.3 から $G=H$ である．このことは G' がGの生成系から除きうることを示している．したがって $\Phi\supseteq G'$ が成立する．有限群に対してはこの逆が成立する．

定理 10.4.4. （**Wielandt**）有限群Gの Frattini 部分群が交換子群 G' を含めばGは巾零群である．

証：PをGのある Sylow 部分群とする．$N_G(P)=H\neq G$ であればHはGのある極大部分群Mに含まれている．$\Phi\subseteq M$ でありまた仮定から $\Phi\supseteq G'$ が成立している．G/G' は可換群であるからMはGの正規部分群となる．一方 $M\supseteq N_G(P)$ であるから定理 4.2.4 によりMはその正規化群に一致することになり矛盾である．したがって $N_G(P)=G$ すなわちGの Sylow 部分群は正規部分群となりGは巾零群となる．

10.5. 超　可　解　群

定理 10.5.1. 超可解群の部分群および商群は超可解群である．

証：Gを超可解群とし $G=A_0\supset A_1\supset A_2\supset\cdots\supset A_r=1$ を各 A_{i-1}/A_i が巡回群であるような不変列とする．商群 $G/K=T$ に対し A_i の準同型像を B_i とすれば $T=B_0\supseteq B_1\supseteq B_2\supseteq\cdots\supseteq B_r=1$ は不変列をなし同じ群を取り去れば巡回

群の任意の準同型像が巡回群か単位群なることから連続した二群 B_{i-1}, B_i は巡回商群 B_{i-1}/B_i をなす．また部分群Hに対し $C_i=H\cap A_i$ と置くと

$$H=C_0\supseteq C_1\supseteq C_2\supseteq\cdots\supseteq C_r=1$$

なる列が得られる．すべての i に対し $H\cap A_i$ はHの正規部分群であって定理 2.4.1 から $C_i/C_{i+1}=H\cap A_i/H\cap A_{i+1}\cong A_{i+1}\cup(H\cap A_i)/A_{i+1}$ が成立する．この右辺は A_i/A_{i+1} の部分群であるから巡回群か単位群である．したがって C_i/C_{i+1} も巡回群か単位群となりHは超可解群である．

系 10.5.1. 超可解群は極大条件を満たす．

超可解群は有限生成であるから定理 10.5.1 によりその部分群も有限生成となり極大条件が満たされることになる．

定理 10.5.2. 超可解群Gはすべての商群 B_{i-1}/B_i が無限巡回群か素数位数の巡回群となるような不変列 $G=B_0\supset B_1\supset B_2\supset\cdots\supset B_k=1$ を持つ．

証：$G=A_0\supset A_1\supset A_2\supset\cdots\supset A_r=1$ を各 A_{i-1}/A_i が巡回群なる不変列とする．$p_1, p_2, \cdots, p_s$ を素数として（必ずしも異ならなくともよい）A_{j-1}/A_j が有限位数 $p_1p_2\cdots p_s$ を持つとすれば A_{j-1}/A_j は位数 $p_1, p_1p_2, \cdots, p_1\cdots p_{s-1}$ の巡回部分群をそれぞれただ一つづつしか含まないからそれらは特性部分群でありそれらに対応する A_{j-1} と A_j の間にある $s-1$ 個の部分群はGの正規部分群であって連続した二群により得られる商群は素数位数の巡回群である．このようにして有限位数の各商群 A_{j-1}/A_j を細分していけば定理に述べられた不変列が得られる．

この定理はさらに改良して素数位数の商群を素数の大小により並べ換えることができる．

定理 10.5.3. 超可解群Gはすべての商群 C_{i-1}/C_i が無限巡回群であるか素数位数の巡回群であって C_{i-1}/C_i, C_i/C_{i+1} がそれぞれ素数位数 p_i, p_{i+1} を持てば $p_i\leqq p_{i+1}$ となるような不変列

$$G=C_0\supset C_1\supset C_2\supset\cdots\supset C_k=1$$

を持つ.

証：$G=B_0\supset B_1\supset B_2\supset\cdots\supset B_k=1$ を定理 10.5.2 で与えられた列とする．もし $B_{i-1}/B_i, B_i/B_{i+1}$ がそれぞれ素数位数 q, p を持ち $q>p$ であるとすれば B_{i-1}/B_{i+1} の位数は $pq(p<q)$ であるから位数 q の特性部分群を持ちその群の完全逆像 B_i^* はGの正規部分群である．B_i を B_i^* で置き換えると B_{i-1}/B_i^* の位数は $p, B_i^*/B_{i+1}$ の位数は q となる．この操作を続けていくとき不変列の長さは変らず最後には素数位数の連続した商群においてその位数が減少しないような列が得られることになる．

系 10.5.2. $p_1\leqq p_2\leqq\cdots\leqq p_r$ を素数としGを位数 $p_1p_2\cdots p_r$ の有限超可解群とすればGは A_{i-1}/A_i が位数 p_i であるような主組成列 $G=A_0\supset A_1\supset\cdots\supset A_r=1$ を持つ.

定理 10.5.4. 超可解群の交換子群は巾零群である.

証：$G=A_0\supset A_1\supset\cdots\supset A_r=1$ を各 A_{i-1}/A_i が巡回群であるようなGの不変列とし $H_i=G'\cap A_i$ と置くと $G'=H_0\supseteq H_1\supseteq\cdots\supseteq H_r=1$ は G' の不変列であってこの列において異なるものだけを取り出すと $G'=K_0\supset K_1\supset\cdots\supset K_s=1$ とかける．ここに K_{i-1}/K_i はすべて巡回群である．これらの K_i が G' の中心列をなすことを示そう．K_i はすべてGの正規部分群の共通部分であるからGの正規部分群である．したがって G/K_i において K_{i-1}/K_i は巡回正規部分群となりGの元による変換は巡回群 K_{i-1}/K_i の自己同型を引き起こす．巡回群の自己同型群は可換群であるから G/K の二元は K_{i-1}/K_i の交換可能な自己同型を引き起こす．したがって任意の二元 x, y の交換子 $x^{-1}y^{-1}xy$ は K_{i-1}/K_i の恒等自己同型を引き起こすことになり K_{i-1}/K_i は G'/K_i の中心に含まれる．したがって K_i は G' の中心列をなすから G' は巾零群となる.

超可解群では任意の部分群の鎖で非常に興味ある性質を持つものがある．ある元 a と，$-\infty$ と $+\infty$ の間の整数全体を動く x に対し $H_1=\sum_x H_2a^x$ が成立するとき H_2 は H_1 において指数 ∞^1 を持つという．したがってもし $A_j\lhd$

A_{j-1} であって A_{j-1}/A_j が無限巡回群であれば a として巡回群 A_{j-1}/A_j の生成元である A_j の剰余類に含まれる任意の元を取れるから A_j は A_{j-1} において指数 ∞^1 を持つ．しかし H_2 が H_1 において正規でなくても H_1 における指数が ∞^1 のこともありうる．

定理 10.5.5. 超可解群Gにおいて部分群の任意の鎖 $G=M_0\supset M_1\supset M_2\supset\cdots\supset M_s=1$ はこの鎖に適当な群を挿入することにより次のように細分することができる．すなわち

$M_{i-1}=M_{i,0}\supset M_{i,1}\supset\cdots\supset M_{i,t}=M_i,\ \ t=t(i),\ \ i=1,\cdots,s$

なる列において $M_{i,j}$ は $M_{i,j-1}$ において素数指数か指数 ∞^1 を持つ．

証：M_1 は超可解であるから $G=M_0$ と M_1 の間に要求されている性質を持った群を挿入して細分化できることを示せば十分である．

$G=A_0\supset A_1\supset A_2\supset\cdots\supset A_r=1$ を各 A_{i-1}/A_i が素数位数か無限位数の巡回群であるような G の不変列とすると $M_1\supseteq A_r=1$, $M_1\not\supseteq A_0=G$ であるから $1,\cdots,r$ の中のある i に対して $M_1\supseteq A_i$, $M_1\not\supseteq A_{i-1}$ が成立する．ここで次の二つに場合を分ける：（1）A_{i-1}/A_i が素数位数を持つ．（2）A_{i-1}/A_i が無限巡回群である．

Case 1. A_{i-1}/A_i が素数位数を持つ．$A_{i-1}\supset M_1\cap A_{i-1}\supseteq A_i$ である．A_i は A_{i-1} において素数指数を持つから A_i と A_{i-1} の間には真部分群は存在しない．したがって $M_1\cap A_{i-1}=A_i$ である．もし $x=0,\cdots,p-1$ のとき $A_{i-1}=\sum_x A_i a^x$ とすれば $M_1\cup A_{i-1}=M_1A_{i-1}=M_1{}^*$ であってかつ M_1 が A_i を含み $a^p\in A_i$ であって元 a を M_1 が含まないから $M_1{}^*=\sum_x M_1a^x$, $x=0,\cdots,p-1$, となり M_1 は $M_1{}^*$ において素数指数を持ち $M_1{}^*\supseteq A_{i-1}$ が成立する．

Case 2. A_{i-1}/A_i が無限巡回群である．$A_{i-1}\supset M\cap A_{i-1}\supseteq A_i$ である．A_{i-1}/A_i の任意の部分群は特性部分群であるから $M_1\cap A_{i-1}$ はGの正規部分群である．もし $M_1\cap A_{i-1}=A_i$, $A_{i-1}=\sum_x A_ia^x$ であるとすれば $M_1{}^*=M_1\cup A_{i-1}=M_1A_{i-1}=\sum_x M_1a^x$ と置くと M_1 は A_i を含むが元 a のどんな巾も含まないか

ら M_1 は M_1^* において指数 ∞^1 を持つ．またもし $M_1 \cap A_{i-1} \supset A_i$ とすると無限巡回群の任意の部分群は有限指数を持つから $M_1 \cap A_{i-1}$ は A_{i-1} において有限指数を持つ．したがって不変列において A_{i-1} と $M_1 \cap A_{i-1}$ の間に群を挿入して各々が直前の群の中で素数指数を持つようにできて Case 1 と同様にして M_1 が素数指数を持つような M_1^* をみつけることができる．これを繰り返していけば鎖 $M_1 \subset M_1^* \subset M_1^{**} \subset \cdots \subset M_1^{(u)}$ であって各群が直後の群の中で素数指数を持ち $M_1^{(u)} \supseteq A_{i-1}$ なるものを見出すことができる．

この操作を続けていけば有限回で $M_1^{(v)} \supseteq A_0 = G$ に到達し定理に要求されている G と M_1 の間の細分がなされる．

この定理は有限群に対しては次のような興味あるかたちでいい表わされる．

定理 10.5.6. 有限超可解群 G において部分群の極大鎖はすべて同じ長さを持ち，もし $p_1, \cdots, p_r$ を素数とし（必ずしも異ならなくてもよい）G の位数が $p_1 p_2 \cdots p_r$ であればその長さは r である．

証：前の定理により極大鎖においてある部分群の直後の群の中での指数はすべて素数であるから鎖の長さは r となる．

系 10.5.1. 有限超可解群の任意の極大部分群は素数指数を持つ．

Huppert [1] によりはじめて証明されたのであるが，この逆が成立することは注目すべきことである．その証明には 16 章で示される群の表現に関する定理のいくつかを使わねばならない．まず P. Hall の未発表の定理を示そう．

定理 10.5.7. **(P. Hall)** 有限群 G がそのすべての極大部分群の指数が素数であるか素数の平方であるという性質（これを性質 (M) とかく）を持てば G は可解群である．

証：G の位数に関する帰納法で示す．p を G の位数を割る最大の素数，S を G の p-Sylow 部分群，N を G の中での S の正規化群とする．もし $N=G$ であれば S は G の正規部分群であって G/S は性質 (M) を満たすから帰納法に

より G/S は可解である．S は p 群であるから G が可解群となる．一方 $N\subset G$ のときは N を含む G の極大部分群 H を選ぶと N は S の G の中での正規化群であると同時に H の中での正規化群でもあるから Sylow の第三定理により $[G:N]=1+k_1p$, $[H:N]=1+k_2p$ が成立しこれらはそれぞれ G および H の中での p-Sylow 部分群の個数である．したがって $[G:H]=1+kp$ が成立する．しかるに仮定から q を素数として $[G:H]=q$ か q^2 であって明らかに $q<p$, $k>0$ が成立するから $kp=q^2-1=(q-1)(q+1)$ が成立する．$p\geqq q+1$ から $p=q+1$ でなければならない．これは $p=3$, $q=2$ のときのみ可能であってこのとき G の位数は 2^a3^b となるから定理 16.8.7 により G は可解である．

定理 10.5.8. **(Huppert)** 有限群 G がそのすべての極大部分群が素数指数を持つという性質（これを (M^1) で表わす）を満たせば G は超可解群である．

証：定理が成立しないと仮定し G を超可解群で性質 (M^1) を満たす群のうち位数が最小の群とする．定理 10.5.7 により G は可解群であるから N を G の極小正規部分群とするとその位数は p を素数として p^α と表わせる．G の最小性により G/N は超可解であって G の主組成列の中で N のみが（連続した二群による商群として）非巡回群である．これから N が G の唯一の極小正規部分群なることが結論される．H/N を G/N の極小正規部分群とすると次の二つの場合に分かれる．(1) $[H:N]=p$,（2）$[H:N]=p$ と異なる素数 q.（1）のとき H は可換群である．なぜならもし可換群でないとすると $1\subset H'\subset N$ であり H' が G の正規部分群となるからである．$\alpha>1$ であるから H は位数 p^2 の元を含まない．なぜならばもし含んだとすれば N は H の位数 p なる特性部分群を含むことになり再び同じ論法により矛盾がえられるからである．したがって H は基本可換群である．

さて G の元は H の自己同型としてすなわち次数 $\alpha+1$ の（H の位数が $p^{\alpha+1}$ であるから）mod. p での一次変換として自然に表現される．H の元 x と，x に無関係な $m=m(a)$ に対し $a^{-1}xa=x^m$ となる G の元 a の全体を K, また H の G 中での中心化群を L とすると K/L は G/L の中心に含まれる．また N

がGの唯一の極小正規部分群でありHの任意の部分群がKの中で正規であるから $K \subset G$ が成立する．ここで M/K を G/K の極小正規部分群とする．もし $[M:K]=p$ とすると位数がpと互いに素で G/L の中心に含まれる K/L と位数pの群 $\{L,a\}/L$ との直積としてM/Lは表わされこのとき $M_1=\{L,a\}$ がGの正規部分群となる．$(N,L)=1$，$[M_1:L]=p$ であるからNは M_1 の中心の単位元以外の元を含まねばならない．M_1 の中心はGの正規部分群であるからNの極小性によりNは M_1 の中心に含まれしたがって $(M_1,N)=1$ が成立する．もし $H=\{N,b\}$ とすると群 (H,M_1) の位数はpであってNの単位元以外の元 $c=(a,b)$ で生成される．この群はGの正規部分群であるからNがGの極小正規部分群ではあり得なくなる．

したがってqをpと異なるある素数として $[M:K]=q$ となるから M/L はpと互いに素な位数を持つ．完全可約性の定理 16.3.1 によりPをMの位数pの正規部分群としたとき $H=N\times P$ が成り立つ．PのGの中での共役はMの中の位数pの正規部分群であってそれらの和QはGの正規部分群である．NがGの唯一極小正規部分群であり $N\neq Q$ なることから $Q=H$ が得られる．PはNに含まれないからPのどの共役もNに含まれない．$P=\{b\}$，$b^p=1$，とし P_i をP以外のPの任意の共役とすると $[H:N]=p$ であるから $PP_i\cap N=R$ は位数pである．$P_i=\{c\}$，$R=\{bc\}$ となるような P_i の生成元cを取ることができる．P,P_i,R はMの正規部分群であるからMの任意の元aに対し $a^{-1}ba=b^m$，$a^{-1}ca=c^n$，$a^{-1}(bc)a=(bc)^t$ が成立する．したがって $(bc)^t=b^mc^n$ から $t=m=n$ となる．しかるに P_i はPの任意の共役であったからHの任意の元xに対し $a^{-1}xa=x^m$ が成立し $m=m(a)$ はxに無関係である．したがって $M\subseteq K$ となり矛盾である．ゆえに（1）の場合は起こり得ない．

（2）の場合はただちに解決される．$[H:N]$ がpと異なる素数qのときQをHの q-Sylow 部分群，TをGの中でのQの正規化群とする．Gの中でのQの任意の共役はHに含まれるからそれはNのある元によるQの共役である．したがって $G=NT$ であって $N\cap T$ はGの正規部分群である．$T\supseteq N$ とすると $T=G$ となりQがGの正規部分群となってしまうから $T\not\supseteq N$ である．したが

って $N \cap T=1$, $[G:T]=p^{\alpha}$ となる．$T \subset T_1 \subset G$ とすると $1 \subset T_1 \cap N \subset N$ であって $T_1 \cap N$ がGの正規部分群であるからTはGの極大部分群である．ゆえにGは素数指数でない極大部分群を持つことになり仮定に反する．

演 習 問 題

1. $I^{(1)}=I^{(1)}(G)$ を群Gの内部自己同型群，$I^{(n)}$ を $I^{(n-1)}$ の内部自己同型群とする．もし列 $G, I^{(1)}, I^{(2)}, \cdots$ の中に単位群があればGは巾零であることを示せ．
2. Gを極大条件を満たす群とする．Gの自己同型群 $A(G)$ が超可解ならばGは超可解であることを証明せよ．
3. a, b を巾零群Gの $a^m=b^n=1$, $(m, n)=1$ なる二元とし $w=a^{-1}b^{-1}ab$ とおく．もし $w \in \Gamma_i(G)$ とすると $w^m \in \Gamma_{i+1}(G)$, $w^n \in \Gamma_{i+1}(G)$ がしたがって $w \in \Gamma_{i+1}(G)$ が成立することを示せ．これから $w=1$ すなわち $ab=ba$ が成立する．
4. 8章の問題2の逆を示せ．すなわちGを有限巾零群，$p_1, p_2, \cdots, p_s$ を積がGの位数であるような素数の任意の順列とするとGは A_{i-1}/A_i が位数 p_i である組成列 $G=A_0 \supset A_1 \supset \cdots \supset A_s=1$ を持つ．
5. Gを $\Gamma_3(G)=1$ なる p 群とする．$G/\Gamma_2(G)$ の元の最高位数を p^m とすると $\Gamma_2(G)$ のどの元も p^m より高い位数を持たないことを示せ．

記　号　表

記号は標準的なものを使う．集合の包含関係の記号：$A \supseteq B$, A は B を含む，$A \supset B$，A は B を真に含む，$A \subseteq B$，A は B に含まれる，$A \subset B$，A は B に真に含まれる；$a \in A$，a は集合 A に属する；$a|b$，a は b を割り切る，$a \equiv b$ (mod. m)，a はmを法として b と合同．一般的な用法として記号の上に線を引いたものはその記号の否定を表わす．したがって，$p \nmid s$，p は s を割り切らない，$y \notin G$，y はGに属さない．

群　論（上）

1969年 8 月15日　第 1 刷発行©
1974年 4 月15日　重 版 発 行

訳　者　金　沢　　稔
　　　　八　牧　宏　美

発行者　吉　岡　　清

京都市左京区田中門前町87
発行所　株式会社　吉　岡　書　店

数 学 叢 書